WI-FI COMO SOLUCIÓN DE CAMPO DE ACCESO LAN, PARA PRESTAR SERVICIOS DE INTERNET Y APLICACIONES, DENTRO DE LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

JAVIER ENRIQUE MARTÍNEZ CORTECERO

JUAN DAVID ZÁRATE TORRES

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

AREA DE POSTGRADOS

CARTAGENA

2004

WI-FI COMO SOLUCIÓN DE CAMPO DE ACCESO LAN, PARA PRESTAR SERVICIOS DE INTERNET Y APLICACIONES, DENTRO DE LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

JAVIER ENRIQUE MARTÍNEZ CORTECERO

JUAN DAVID ZÁRATE TORRES

Monografía para optar al título de

Ingenieros electrónicos con Minor en Comunicaciones y Redes

Director

Francisco Jiménez

Ingeniero Promigas Telecomunicaciones

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

AREA DE POSTGRADOS

CARTAGENA

2004

Nota de aceptación

Firma de presidente del jurado

Firma del Jurado

Firma del jurado

Cartagena, Junio de 2004

Dedico éste triunfo:

A mi gran amada madre que ha colocado todas sus fuerzas, sobre procelosos caminos para permitirme conseguir éste nuevo, de muchos más triunfos que compartiré junto a mis hermanos. Este logro también quiero dedicarlo a mi tía Judith, que ha sido mi segunda madre en victorias y derrotas. A mi inolvidable esposa, que desde la distancia siempre llena los más intrincados momentos de esperanza y comprensión.

Mis dedicatorias, a un nuevo ser que desde muy pronto será también parte de mis triunfos, por que hacia él van dirigidos para embelecarlo con el grito de la victoria desde ahora para su mejor educación.

A toda mi familia no me queda más que expresarles lo refocilado que me siento por su apoyo, dedicando también éste trabajo que juntos hemos conseguido.

Javier Enrique Martínez Cortecero

Dedicatoria:

Este trabajo se lo dedico en primera instancia a las personas que han confiado en mi durante este largo trayecto de mi vida, y que han puesto sus esfuerzos para mi surgimiento como persona integra y apta para servirle a la sociedad, estas personas son mis padres José A. Zárate D. Y Mariela Torres V. a los cuales gracias a Dios debo mi vida, también a mis hermanos y demás familiares y amigos cercanos que me han acompañado en la ardua labor.

Juan David Zarate Torres

Agradecimientos a:

Dios, por permitirme estar despierto cada día, a mi madre y toda mi familia por el apoyo incondicional que me han brindado. Gracias a mi director Francisco Jiménez por sus calurosas frases de apoyo y en especial a los ingenieros Roberto Almanza y Enrique Khaléd Daza por que sin ellos éste proyecto no sería tan glorioso.
Gracias a mi compañero Juan David, por saber llevarme en circunstancias difíciles y devolverme a la calma; para todos...
¡Este trofeo es por ustedes!

Javier Enrique Martínez Cortecero

Agradecimientos a:

Gracias a Dios que es mi fuente de toda inspiración y la fuerza que me da vida. A mis padres y a mi familia por poner todo su apoyo en mi y por esperarme mientras terminaba este trabajo. A mi asesor y director de monografía Francisco Jiménez , a mis amigos Ingenieros Enrique Khaled y Roberto Almanza, quienes además de proponerla, pusieron todo su empeño en el desarrollo y mejoramiento de la monografía y por supuesto a mi compañero de monografía Javier Martinez por estar con migo en esto. De corazón ; MUCHAS GRACIAS ¡¡¡¡¡

Juan David Zárate Torres

Cartagena D. T. y C., Junio de 2004

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS DE GRADO.

Universidad Tecnológica de Bolívar

La Ciudad

Respetados Señores:

Con toda atención, nos dirigimos a ustedes, con el fin de presentarles a su consideración, estudio y aprobación, la Monografía titulada **"WI-FI COMO SOLUCIÓN DE CAMPO DE ACCESO LAN, PARA PRESTAR SERVICIOS DE INTERNET Y APLICACIONES, DENTRO DE LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR"** como requisito parcial para optar al Titulo de Ingeniero Electrónico.

Atentamente,

_____ _____

Javier Enrique Martínez Cortecero **Juan David Zárate Tórres**

Cartagena D. T. y C., Junio de 2004

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS DE GRADO.

Universidad Tecnológica de Bolívar

La Ciudad.

Cordial saludo.

A través de la presente me permito entregar la monografía titulada **"WI-FI COMO SOLUCIÓN DE CAMPO DE ACCESO LAN, PARA PRESTAR SERVICIOS DE INTERNET Y APLICACIONES, DENTRO DE LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR"**, para su estudio y evaluación, la cual fue realizada por los estudiantes JAVIER ENRIQUE MARTÍNEZ CORTECERO y JUAN DAVID ZARATE TÓRRES del cual acepto ser su director.

Atentamente,

_____

Francisco Jiménez Castilla
Ingeniero Electrónico.

AUTORIZACIÓN

Cartagena D. T. y C., Junio de 2004

Yo **Javier Enrique Martínez Cortecero**, identificado con cédula de ciudadanía 73.187.561 de la ciudad de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de Monografía y publicarlo en el catálogo online de la Biblioteca.

_____

JAVIER ENRIQUE MARTÍNEZ CORTECERO

AUTORIZACIÓN

Cartagena D. T. y C., Junio de 2004

Yo **Juan David Zarate Torres**, identificado con cédula de ciudadanía 17'958.288 de Fonseca (Guajira), autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de Monografía y publicarlo en el catálogo online de la Biblioteca.

_____

JUAN DAVID ZARATE TORRES

CONTENIDO **Paginas**

LISTA DE TABLAS

Paginas

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ANEXOS

GLOSARIO

Administración de red: Término genérico que se usa para describir sistemas o acciones que ayudan a mantener y caracterizar una red o resolver problemas de la red.

AES: acrónimo del Estándar de cifrado avanzado; que es un estándar de los Estándares de procesamiento de información federal (FIPS de Estados Unidos) y específicamente se refiere a la publicación 197 de FIPS, la que específica un algoritmo criptógrafo que se debe usar por organizaciones gubernamentales a fin de proteger información sensible y no confidencial. Los expertos de seguridad normalmente están de acuerdo en la adopción de éste estándar para entidades comerciales y compañías de desarrollo de redes.

Algoritmo: Una regla bien definida o proceso para llegar a la solución de una problema.

Amplitud: La magnitud o fuerza de una forma de onda variable.

Ancho de banda: Rango de frecuencias necesario para transportar una señal, medido en unidades de hertz. Por ejemplo, las señales de voz requieres aproximadamente 7 kHz de ancho de banda, así como el tráfico de datos requiere 50 kHz, pero esto depende del esquema de modulación, velocidad de datos y la capacidad de canales del espectro de radio que se usen.

ANSI: Acrónimo de Instituto nacional de estándares de estados Unidos. Una organización voluntaria compuesta de miembros corporativos, gubernamentales y

de otros tipos que coordina las actividades relacionadas con los estándares, aprueba los estándares naciones de USA y desarrolla posiciones en las organizaciones de estándares internacionales. ANSI ayuda a desarrollar estándares internacionales y de la Unión Americana relacionados con, entre otras cosas, las comunicaciones y las redes. ANSI es un miembro de IEC e ISO.

Antena: Un dispositivo para transmitir y/o recibir una frecuencia de radio (RF), por lo común, las antenas están diseñadas para frecuencias específicas y definidas de manera relativamente estricta, por lo que su diseño varía mucho de acurdo al sistema.

AP: Acrónimo de punto de acceso. Un punto de acceso es un dispositivo que normalmente conecta a los dispositivos de cliente, por ejemplo, tarjetas PCMCIA, con la porción Ethernet de una LAN. Normalmente un punto de acceso tiene un puerto Ethernet y otro de energía en la parte trasera e incluso una o dos antenas que transmiten y reciben señales RF de los dispositivos de cliente, otros puntos de acceso o puentes de grupos de trabajo.

ARP: Acrónimo del protocolo de resolución de direcciones. Un protocolo de la Capa 3 del modelo OSI que se usa para asignar direcciones de red IP a las direcciones de hardware que usa el protocolo de enlace de datos de la Capa 2. El protocolo funciona cuando se transporta IP a través de Ethernet.

ARQ: Acrónimo de la solicitud de repetición automática. Una técnica de comunicación en la que el dispositivo receptor detecta errores y solicita retransmisiones.

ASCII: Acrónimo del Código estándar de Estados Unidos para el intercambio de información. Específica un código de 8 bits para la representación de caracteres (7 bits más la paridad).

Atenuación: La pérdida de energía en la señal de comunicación, ya sea por el diseño del equipo, manipulación del operador o transmisión a través de un medio, por ejemplo, la atmósfera, cobre o fibra.

Autenticación: En seguridad, la verificación de la identidad de una persona o proceso.

Autenticación abierta: Un tipo de autenticación donde un AP concede la autenticación a cualquier cliente, sin importar si pertenece o no a la red ese AP en particular. Se puede decir que más común en los dispositivos de datos sencillos, por ejemplo, los lectores del código de barras que tienen poco pode de procesamiento.

Autenticación de estación: El proceso de autenticar un dispositivo 802.11, por ejemplo, un punte o AP, a diferencia de autenticar un cliente, como una tarjeta PCMCIA.

Banda ancha: En general describe un sistema de datos que tiene velocidad de información constante de, o superior a, 1.5 Mbps. Su opuesto correspondiente es la *banda angosta*.

Banda base: Características de una tecnología de red donde sólo se usa un portador de frecuencia. Ethernet es un ejemplo de una red de banda base. También se conoce como *banda angosta*.

Bandas ISM: normalmente, pero no siempre, se acuerda que las bandas industriales, científicas y médicas son las siguientes: 902 a 928 MHz, 2.4 a 2.485 GHz, 5.15 a 5.35 GHz y 5.725 a 5.825 GHz.

Baudio: Unidad para señalar la velocidad igual al número de elementos de señal discretos transmitidos por segundo. Baudio es un sinónimo de bits por segundo (bps) si cada elemento de señal representa exactamente un bit.

BBFW: Acrónimo de los sistemas inalámbricos fijos de banda ancha. En general, implica transferencia de datos por encima de 1.5 Mbps.

Canal adyacente: un canal o frecuencia que está directamente encima o debajo de un canal o frecuencia especifica.

CDMA: Acrónimo de acceso multiplexado por división de código. Esquema de transmisión que permite que múltiples usuarios compartan el mismo rango de frecuencias RF.

CLI: Interfaz de línea de comando. Por medio de esta, los técnicos de red controlan los parámetros reales el radio. Reside en los routers o switches que se encuentran en cada extremo de BBFW.

CRC: Acrónimo de revisión de redundancia cíclica. Es una técnica de revisión de errores en la que la trama que se recibe calcula un valor restante al dividir el contenido de la trama mediante un divisor binario principal y compara el valor restante calculado con un valor que el nodo emisor almacena en la trama.

DES: Acrónimo de estándar de cifrado de datos. Un algoritmo de cifrado estándar que usa la agencia nacional de estándares de Estados Unidos. En términos de redes DES se conoce como estación final de destino.

DNS: Sistema de nombre de dominio.

Dominio: Una agrupación general de LAN basadas en un tipo de organización o área geográfica.

DSSS: Acrónimo del espectro extendido de secuencia directa. Técnica de propagación en la que distintas señales de información transmiten por un conjunto de frecuencias especifico de manera secuencial desde la frecuencia más baja hasta la más alta.

EAP: acrónimo de Protocolo de autenticación extensible

EAP-TLS: acrónimo de protocolo de autenticación extensible-seguridad a nivel de transporte.

FDM: Acrónimo de la Multiplexión por división de frecuencia. El esquema de modulación que divide el espectro disponible total en subconjuntos, mismos que normalmente se usan en paralelo a través de uno o más enlaces.

ISP: Acrónimo de Protocolo servicios de Internet. Un ISP es un proveedor de acceso a Internet, por ejemplo, Airlink, MSN o AOL.

PDU: acrónimo de la unidad de datos de protocolo. El término OSI para paquetes.

PEAP: Acrónimo del protocolo de autenticación protegida extensible. Proporciona la autenticación mutua y la generación de claves, de manera que la fase de autenticación del usuario esta protegida.

QAM: Acrónimo de la modulación de amplitud de cuadratura. Método de modulación de señales digitales que se relaciona con la amplitud y el código de fase.

SSID: Acrónimo de identificador de establecimiento de servicio. Un ID que permite la separación lógica de WLAN.

WEP: Acrónimo del protocolo equivalente al cableado. Protocolo de seguridad usado en 802.11 para proteger las comunicaciones inalámbricas.

RESUMEN

Las tecnologías de redes inalámbricas LAN disponibles en el mercado, son muchas y cada vez seguirán emergiendo, por la gran demanda que se está presentando. Aquí se comparan dichas tecnologías de manera que se haga la selección de una apropiada red para su implementación en la universidad. Se hace un estudio de todos los componentes teóricos de la tecnología seleccionada (Wi-Fi), los cuales conllevan condiciones de operación que son útiles en el desarrollo del diseño de una red de comunicaciones con características de confiabilidad y accesibilidad, que define todas las directrices que satisfacen las necesidades de los usuarios en donde lo requieran dentro de la UTB.

La seguridad y la calidad de servicio, que ya están estandarizadas por la IEEE 802.11, son dos puntos muy a priori, ya que éstas son las que le dan la mayor parte de la confiabilidad de las redes de datos.

Por último, se darán las pautas principales para determinar nuestro diseño como solución de acceso LAN.

En el capítulo uno se mencionan los principales tipos de redes que existen, fijas o cableadas e inalámbricas, y luego se hace una comparación entre estas

desatacando sus ventajas y desventajas, con el fin de justificar la migración desde las redes cableadas, hacia las redes inalámbricas.

Complementando la intención del capítulo uno de familiarizarnos con las redes, en el capítulo dos se comienza a definir lo que son las redes inalámbricas como tal comenzando desde su historia y definición hasta su clasificación en redes publicas de radio, redes de área local, redes infrarrojas y redes de radio frecuencia.

Luego de estudiar las redes inalámbricas de forma general, se comienza a profundizar en las redes de radiofrecuencias en el capítulo tres, donde se distinguen cuatro de las tecnologías inalámbricas que usan RF con mas auge en el mercado, como lo son Bluetooth, Hiperlan, HomeRF y la familia de IEEE 802.11, definiendo en cada una sus características para la transmisión de la información como, arquitectura de red, velocidad de datos, rango de frecuencias de operación y alcance en distancia o cobertura.

A partir del capítulo cuatro se dejan atrás las clasificaciones y se comienza a profundizar en Wi-Fi basado en 802.11b que fue la tecnología seleccionada por sus características que concuerdan con el entorno de la UTB. Se describen factores como la topología de red que utiliza, de igual manera, se describe su capa física y su capa de enlace, describiendo funciones que son posibles en la capa de enlace de los dispositivos Wi-Fi como; la exploración, la autenticación, la

asociación, la seguridad, y algunos modos de operación que complementan y mejoran las prestaciones de estos dispositivos como lo son, el modo RTS/CTS, el modo de ahorro de energía, la fragmentación y el roaming.

En el capítulo cinco se describen dispositivos que se usan en los despliegues Wi-Fi, como lo son los puntos de acceso (AP), los puentes o bridges (que para nuestro diseño no serán tenidos en cuenta pero se añaden como información de su existencia), los repetidores, los routers y los gateways.

Un capítulo muy importante en la monografía, es el seis en donde se analizan detalladamente las características que afectan o aportan al desempeño de los dispositivos Wi-Fi 802.11b, como lo son las diferentes velocidades que manejan y la forma de obtenerlas, los factores que afectan en la capacidad de salida como la sobrecarga con respecto a la carga, los factores que influyen en el rango o alcance de los AP y dispositivos clientes Wi-Fi como, la potencia de transmisión, la selección de una antena específica, las limitaciones de la propagación RF, diversidad de antenas, perdidas en los cables y la interoperabilidad entre dispositivos Wi-Fi.

Definitivamente el talón de Aquiles de nuestra red es la seguridad, debido a las características del medio de transmisión, que es un medio abierto a cualquier intruso que puede alterar las transacciones normales de la red Wi-Fi. Para esto en

el capítulo siete se describen técnicas para cifrar la información de la red donde sea hace necesario que el usuario sea autenticado por un servidor de autenticación, estas técnicas tienen origen en el protocolo WEP (Protocolo equivalente al cableado), el cual sienta las bases para otras técnicas mas avanzadas como el estándar 802.11i.

Otro factor de mucha importancia para considerar en la instalación de una red Wi-Fi, es proporcionar satisfacción a los usuarios a la hora en que estos utilicen sus servicios. El capítulo ocho, nos muestra la forma de hacer, proporcionar calidad de servicio QoS fundamentada en el estándar 802.11e. Se hace una clasificación del trafico sensible al tiempo, para luego darle niveles de prioridad. Esto es posible mediante el uso de estándares como el 802.1Q y 802.1D, que establecen el uso de etiquetas para diferenciar la información.

A manera de información y de complementación de los temas tratados en la monografía, en el capítulo nueve, estudiamos la posibilidad de utilizar Wi-fi en la ultima milla de un sistema de comunicaciones y las consideraciones practicas que conlleva esto.

Por último, el capítulo diez, describe completamente el despliegue de la red Wi-Fi en la UTB, teniendo en cuenta las consideraciones de los capítulos anteriores, y además, realizando un estudio de las áreas de la universidad, se hace un

presupuesto o planeación de capacidad o ancho de banda para los usuarios, se determina la cobertura de la red Wi-Fi en la UTB haciendo una evaluación en el sitio, luego se hace un estudio del diseño de exteriores e interiores en la universidad, se ubican los puntos de acceso y se selecciona su fabricante. También se explica como administrar la red Wi-Fi de la UTB, como se mantiene y se supervisa su infraestructura.

Se llego a la conclusión, de que para dar conexión a usuarios que se encuentren en exteriores dentro e la universidad, solo se necesita un solo AP Wi-Fi 802.11b que irradie energía de 2.4 GHz con una potencia de 100 mW en todas las direcciones en un radio de 240 m (suficiente para cubrir toda la universidad), con el uso de una antena omnidireccional, ubicada en el techo de malockanet. Los tres AP adicionales que se colocan en la red se usan como repetidores que reforzaran la señal en lugares interiores, como la biblioteca, rectoría, donde se dificulta la recepción de la señal del AP principal. Para la seguridad de la red se utiliza el protocolo WEP con claves de autenticación dinámicas para imposibilitar la alteración de la información por parte de intrusos. La calidad de servicio se asigna utilizando niveles de prioridad para los usuarios mas importantes de la red.

INTRODUCCIÓN

La optimización de las redes de comunicaciones en las empresas ya es mas que un boato tecnológico, ¡es una realidad!.

Las empresas están teniendo un enorme desajuste por el glorioso avance de las tecnologías de redes y es cada vez menor, el tiempo de duración de las estructuras cableadas para redes de datos; lo que está llevando a todo el sector a buscar nuevas formas de minimizar sus costos con infraestructuras que perduren mas en tecnologías. Es aquí donde nace el concepto de redes inalámbricas.

El origen de las Wireless LAN se remonta al año 1979, cuando ingenieros de IBM en Suiza publicaron los resultados de un experimento que consistía en utilizar enlaces infrarrojos para crear una red de área local en una fábrica. Puede considerarse que el punto de partida en la línea evolutiva de las tecnologías inalámbricas, se debe a esos resultados publicados en el volumen 67 de los Proceeding del IEEE.

Las WLAN han surgido como una opción dentro de la corriente hacia la movilidad universal sobre la base de una filosofía "seamless" o sin discontinuidades, o sea, que permita el paso a través de diferentes entornos de una manera transparente.

La aparición en el mercado de los laptops y los PDA (Personal Digital Assistant), y en general de sistemas y equipos de informática portátiles es lo que ha generado realmente la necesidad de una red que los pueda acoger, verbigracia, las LAN inalámbricas. De esta manera, la WLAN hace posible que los usuarios de ordenadores portátiles, puedan estar en continuo movimiento, al mismo tiempo que están en contacto con los servidores y con los otros ordenadores de la red, es decir, ésta tecnología permite movilidad y acceso simultáneo a la red.

Una LAN inalámbrica puede definirse como una LAN que utiliza tecnología de radiofrecuencia para enlazar los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas.

Los gastos en Tecnología Inalámbrica, hoy en día tienen que ver menos con la implementación de nuevas tecnologías y más con mejoras de rendimiento, confiabilidad y operación del equipo que ya está instalado, para poder cumplir con los objetivos de las empresas y minimizar sus gastos futuros, por el crecimiento exponencial de las nuevas tecnologías.

Las empresas están planeando crear redes con tecnologías fácilmente expansibles, en vez de pagar por equipos que son limitantes o que pierden valor. Un ejemplo de optimización de redes es la liberación de capacidades avanzadas

en la red para soportar nuevas aplicaciones habilitadas a través de la Web, que resulten en mayor productividad.

La modernización y la simplificación de la administración de la red también es otro ejemplo muy claro, que evita problemas que, de otro modo, causarían incrementos en los costos operacionales.

Un tercer ejemplo sería un cliente que apro vecha la tecnología ya existente para acomodar a más empleados o más requerimientos de tráfico de red. En fin, ante las múltiples aplicaciones de las Wireless LAN y sus ventajas sobre las redes cableadas; las empresas y corporaciones industriales se están viendo tentadas por éstas tecnologías.

Actualmente, los gerentes de redes usan formas más creativas para obtener mayor valor de sus recursos existentes. "Los usuarios adoran la tecnología moderna, pero estos días están más interesados en estirar sus presupuestos. Los productos y servicios que ofrecen beneficios inmediatos, tales como mejor seguridad o costos operativos más bajos, florecen desde el 2003"[1]. Por esto desde ese año, la necesidad de adoptar tecnologías inalámbricas en las empresas, ha

[1] De acuerdo al reporte de Forrester Research titulado "Infraestructura americana del Norte: sinopsis de la tecnografía empresarial (*Infrastructure North America: Business Technographics Overview*)" realizado en octubre del 2002.

provocado un cambio drástico, al pasar de ser una moda, como lo fue en el 2002, a ser algo esencial.

Nuestra investigación sobre las redes inalámbricas genera un gran interés para suplir las tendencias de las empresas y también permite a los interesados en el campo a adelantar sus investigaciones y profundizar con las nuevas tecnologías emergentes sobre redes inalámbricas que pronto incrementarán su demanda en el mercado.

La prueba de esta tendencia yace en el continuo crecimiento en compras de WLANs empresariales, a pesar de las problemáticas condiciones económicas que se han levantado en todas partes. Las WLANs son una de las pocas áreas tecnológicas donde las empresas todavía están haciendo gastos considerables. Es que definitivamente no queda duda de que las redes Wireless están llenando de grandiosos beneficios a las empresas y que se tiene aun mucho fruto por recogerse de ellas.

De acuerdo a un reporte de Gartner Dataquest, titulado "El mercado de las LANs Inalámbricas preparado para un crecimiento sólido hasta el 2005"[2] *(Wireless LAN Market Set for Strong Growth Through 2005*), los gastos de los usuarios finales en

[2] Gartner Dataquest espera que el mercado mundial crezca a una tasa anual compuesta de un 22 por ciento hasta el 2005.

productos de LANs Inalámbricas aumentaron en el 2001 en un 40 por ciento a 1.5 billones de dólares en todo el mundo. Esto principalmente por el tema de la seguridad, mejor llamado “Seguridad en niveles”, ya que las empresas buscarán cada vez más la forma de proveer una protección máxima de seguridad en múltiples niveles y puntos de acceso a la red.

La razón es simple; el acceso inalámbrico le permite a los empleados acceder a la información de forma rápida y segura desde cualquier lugar en la empresa, fomentando una toma más rápida de decisiones en base a un acceso a información ilimitada, ya sea en bases de datos corporativas o el Internet. Gartner Dataquest reportó que “el impulsor principal” de las LANs Inalámbricas es “la creciente demanda de ancho de banda para permitir que las computadoras portátiles tengan acceso más flexible al e-mail, contenido en la Web y aplicaciones corporativas”. Actualmente, las redes locales inalámbricas (WLAN) se encuentran instaladas mayoritariamente en algunos entornos específicos, como almacenes, bancos, restaurantes, fábricas, hospitales y transporte. Las limitaciones que, de momento, presenta esta tecnología ha hecho que sus mercados iniciales hayan sido los que utilizan información tipo "bursty" (períodos cortos de transmisión de información muy intensos seguidos de períodos de baja o nula actividad) y donde la exigencia clave consiste en que los trabajadores en desplazamiento puedan acceder de forma inmediata a la información a lo largo de un área concreta, como

un almacén, un hospital, la planta de una fábrica o un entorno de distribución o de comercio al por menor; en general, en mercados verticales.

Wi-Fi; es una de las tecnologías con mayor acogida de la industria, por la expansión en metros que brinda su cobertura. Por esto realizaremos un diseño para la Universidad Tecnológica de Bolívar de red Wi-Fi, que maneja el estándar 802.11b, el cual trabaja en el espectro de frecuencias de los 2.4 GHz. En el diseño incluiremos la calidad de servicio, tanto para el cliente como para el proveedor.

Esta red para la tecnológica, les prestará a profesores, estudiantes y demás empleados del campus de ternera, movilidad absoluta sin perder la conexión a otros portátiles, bases de datos y sobre todo al acceso a Internet, desde cualquier lugar dentro de la cobertura que brindan los “puntos de acceso” en la red.

OBJETIVO GENERÁL

Complementar y mejorar el sistema de comunicación actual de la Universidad Tecnológica de Bolívar, permitiendo la movilidad de los puestos de trabajo de estudiantes y profesores, para hacer más constantes y productivas sus actividades académicas e investigativas, dentro del campus.

OBJETIVOS ESPECÍFICOS

- Definir y diferenciar las redes de comunicación existentes, para conocer el funcionamiento de una más específica, como es nuestro caso, las inalámbricas de radio frecuencias, utilizadas por Wi-Fi.
- Distinguir las diferentes tecnologías de tipo LAN inalámbricas, estudiar sus características y evolución, para destacar la tecnología a utilizar (Wi-Fi).
- Seleccionar cuál es la mejor tecnología LAN inalámbrica que se puede utilizar para las instalaciones del campus ternera de la UTB, explicar su estructura, y los elementos que la conforman.
- Identificar y describir los diferentes parámetros que afectan en el funcionamiento y desempeño en cuanto a capacidad de salida y rango o cobertura de los dispositivos que interactúan en la red Wi-Fi 802.11b de la UTB.
- Encontrar la mejor forma de asegurar nuestra red Wi-Fi, de personas no autorizadas para el uso de la red, sin disminuir el rendimiento de esta.
- Examinar las diferentes formas que existen para brindar calidad de servicio QoS a nuestra red, por medio del estándar 802.11e para que el usuario experimente velocidades de datos optimas en sus transacciones.
- Reunir los parámetros necesarios para hacer un diseño de la red de comunicaciones de la UTB, para brindar cobertura a la mayoría de los

usuarios que cumplan con los requisitos para hacer parte de esta, para el acceso a Internet e información ínter-universitaria, en la Universidad.

1. GENERALIDADES, REDES DE DATOS

1.1 Clasificación de las redes de datos

Antes de entrar a fondo en las redes inalámbricas haremos una sucinta descripción sobre todas las redes de datos, en cuanto a su clasificación

Según la naturaleza del medio de soporte físico para el transporte de la información, Las redes se podrían dividir en:
Fijas (por cableado estructurado o fibra, fundamentalmente).
Y las inalámbricas (emisiones de radio u ópticas por medio aéreo).

1.2 Las Redes inalámbricas frente a las Redes fijas

Las redes inalámbricas no sólo tienen cabida en entornos en los que es mandatario una solución inalámbrica. Contrariamente a lo que se piensa, una de sus grandes ventajas radica en su empleo como red fija, pues son múltiples los beneficios que ofrecen frente a la instalación de cableado estructurado convencional. Es esta una faceta todavía relativamente desconocida pero que puede reportar un fuerte impulso a su introducción en el ambiente empresarial y residencial. Se puede aplicar tanto a redes de área local (LANs) dentro de la empresa como en la interconexión de redes de edificios próximos, en la que la solución cableada requiere complejas tramitaciones o es obligada la

contratación de la línea de datos a un operador de red con licencia para operar públicamente.

A continuación se analizarán en detalle los aspectos en las que dichas redes aventajan a las fijas:

Economía: El coste de despliegue de una WLAN puede estimarse entre 75 y 150 € por puesto de trabajo (cableado y puntos de acceso, sin contar con los adaptadores de usuario), dependiendo notablemente de los requerimientos (seguridad, calidad, bitrate) y de las características del lugar de implantación. En el caso de una red cableada, el coste puede oscilar entre 100 y 400 €, donde la gran dispersión en el presupuesto se atribuye fundamentalmente a la problemática asociada al despliegue físico del cableado. Mientras que en plantas especialmente preparadas con falsos techos y/o suelos el coste de ambas soluciones puede estar próximo, en aquellos en los que no exista dicha pre-infraestructura ofimática[3] y máximo si hay materiales costosos (madera, piedra, cerámicos) en suelos, paredes y techos, el precio de la solución cableada se dispara. Existen algunos escritos, consecuencia de estudios realizados por entidades universales que afirmas que las "Wireless LAN pueden economizar más del 80 por ciento, frente a las redes cableadas"[4].

[3] Automatización mediante sistemas electrónicos, de las comunicaciones y procesos administrativos en las oficinas.
[4] Recientemente Toshiba España publico un estudio en el que va todavía muy lejos en cuento a la economía de las WLANs, llegando a afirmar que la reducción de costes por la implantación de una red inalámbrica puede suponer ahorros de hasta un 95% frente a un despliegue tradicional.

Rapidez de implantación: Por lo general la tarea que suele consumir mayor tiempo en la instalación de una red inalámbrica es paradójicamente la parte cableada que se emplea para enlazar los puntos de acceso con la red local de la empresa. Aún así se mide en días la duración de un proyecto, siempre dependiendo de su envergadura. En el caso de redes fijas, no son días sino habitualmente semanas. Esto es en muchos casos un factor decisivo para ciertos proyectos. También cada vez se ven más casos de exhibiciones primeras o ampliaciones de infraestructura que por necesidades urgentes se inician por la construcción de una red wireless para posteriormente consolidarse con una cableada, aunque manteniendo la primera para temas de movilidad y atender los requerimientos de ciertos usuarios.

Movilidad: Es patente que este es el punto fuerte de las WLANs, inalcanzable para las cableadas. Es especialmente interesante para cubrir salas de reunión, laboratorios, centros itinerantes[5], donde haya portátiles y en general para facilitar reuniones de trabajo en cualquier punto. La movilidad en el hogar también es un valor en alza, pues permite que ese portátil sea ubicuo.

Estética: Las instalaciones de redes locales se caracterizan por la existencia de infinidad de rosetas (cajas de conexiones) próximas a cada puesto de trabajo, canalizaciones generalmente visibles y cables desde los PC's hasta el punto de conexión más próximo. Todo ello y debido a la cada vez mayor densidad de

[5] Ambulantes, que se mueven de un lugar a otro.

equipos, impacta de forma muy negativa en la estética del entorno de trabajo. Como contrapartida, en una instalación wireless desaparecen los cables de los PC's y las rosetas, así como se reducen al mínimo las canalizaciones visibles. Este factor, siempre bien valorado, en ocasiones se convierte en fundamental, decidiendo la tecnología de la red a implantar.

Provisionalidad: Las WLANs tienen una gran utilidad en instalaciones que tienen carácter de provisionalidad. Ejemplos de ello son infraestructuras itinerantes (ferias, congresos, demostradores), despliegues cortos o limitados en el tiempo (oficinas temporales), para absorber fuertes picos de utilización ocasional (las WLAN pueden soportar un número elevado de usuarios transitorios, mientras que las fijas están limitadas a las conexiones ya cableadas exclusivamente) y para permitir crecimientos urgentes en una red ya establecida hasta adoptar otras alternativas. Las razones que soportan esta característica frente a la solución cableada son múltiples: economía, escalabilidad, rapidez de implantación, movilidad, etc.

Robustez: Las redes basadas en cableado estructurado son por lo general más robustas frente a interferencias y condiciones adversas que las inalámbricas. Sin embargo en ciertos entornos en fábricas con elevada humedad, agentes químicos agresivos, calor, etc. las instalaciones cableadas pueden sufrir una rápida degradación o ser inviables. Incluso ante situaciones inesperadas que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa,

hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances. Una instalación wireless adecuadamente ubicada para resguardarse de dichas inclemencias puede ser la alternativa idónea.

Obviamente no todas son ventajas de las redes inalámbricas frente a las cableadas; hay una serie de parámetros en las que las últimas ofrecen mayores prestaciones. La velocidad binaria es mucho mayor, obteniéndose en general límites máximos de 100 Mbps por puesto (fast ethernet) frente a 54 Mbps en una WLAN (802.11g) compartidos entre varios usuarios. Son asimismo más inmunes a interferencias, más seguras y requieren de un menor mantenimiento. Estas desventajas pueden ser realmente importantes o casi insignificantes dependiendo de la aplicación que se requiere en cuanto a la calidad de la implantación.

1.3 Inconvenientes de las Wireless

Los principales inconvenientes de las WLANs se ven resumidos en los siguientes ítem.

Calidad de Servicio: Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 54 Mbps (802.11g), frente a los 100 Mbps (fast ethernet) que puede alcanzar una red normal y corriente. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias. Esta se puede situar alrededor de 10^{-4} frente a las 10^{-10} de las redes cableadas. Esto significa que hay 6 órdenes de magnitud de diferencia y eso es mucho. Estamos hablando de 1 bit erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

Soluciones Propietarias: La estandarización hasta ahora es que anda marchando un poco más rápida, por esto ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de enlace, etc. Pero vale aclarar que esto ya no es tan relevante por que los estándares ya están manejando éste factor muy detalladamente.

Después de analizar todos los factores mencionados anteriormente la solución inalámbrica es la elección. Por lo tanto en las paginas siguientes abarcaremos solo las tecnologías inalámbricas existentes partiendo desde su historia hasta su funcionamiento y aplicaciones en las comunicaciones.

2 REDES INALÁMBRICAS

2.1 Introducción

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

Sería exagerado decir hoy que una red inalámbrica remplace a la actual red cableadas, pero esto en pocos años ya podríamos estar reconsiderándolo. Ya que las redes actuales ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica; pero así mismo no sabemos lo que puedan hacer los empresarios de redes en los próximos años, por eso dejaremos abierta la afirmación anterior.

Sin embargo, hoy podemos mezclar las redes cableadas y las inalámbricas, y de esta manera generar una “Red Híbrida” y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

2.2 Historia de las redes inalámbricas

Los primeros experimentos realizados con redes inalámbricas se dieron en 1979 en manos de científicos de IBM en Suiza, quienes implementaron la primera red de importancia con tecnología infrarroja. Continuaron con experimentos con microondas utilizando el esquema spread-spectrum (altas frecuencias).

Es así como en 1985 inicia la comercialización de estas redes, y la FCC[6], asigna un conjunto de bandas estrechas de frecuencia para uso libre en los 2,4 y los 5 GHz. Bandas IMS (Industrial, Scientific and Medical): 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para las redes inalámbricas basadas en spread-spectrum.

Luego para esa misma época la IEEE (Asociación de ingenieros eléctricos y electrónicos), organizo una comisión de trabajo para desarrollar un estándar para esta tecnología de red en dichas bandas; el estándar 802.11, y a partir de este han aparecido estándares mejorados y diferentes, el ultimo de ellos es el 802.11g y ya se está hablando de que en el año 2005 podría salir el estándar 802.11n.

[6] Órgano regulador del espectro radioeléctrico americano

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria. Ese respaldo hizo que las redes inalámbricas empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLANs operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

2.3 Clasificación de las redes inalámbricas

Las redes inalámbricas también entran dentro de las clasificaciones definidas para las redes de datos en cuanto a la cobertura, pero aquí las clasificamos en las siguientes categorías:

2.3.1 Redes públicas de radio

Las redes públicas tienen dos protagonistas principales: "*ARDIS*" (una asociación de Motorola e IBM) y "Ram Mobile Data" (desarrollado por Ericcson AB, denominado *MOBITEX*). Este ultimo es el más utilizado en Europa. Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia. La compañía proporciona la

infraestructura de la red, se incluye controladores de áreas y Estaciones Base, sistemas de cómputo tolerantes a fallas, estos sistemas soportan el estándar de conmutación de paquetes X.25, así como su propia estructura de paquetes. Estas redes se encuentran de acuerdo al modelo de referencia OSI; ARDIS especifica las tres primeras capas de la red y proporciona flexibilidad en las capas de aplicación, permitiendo al cliente desarrollar aplicaciones de software Por ejemplo: Una compañía llamada RF Data, desarrollo una rutina de compresión de datos para utilizarla en estas redes públicas). Los fabricantes de equipos de computo venden periféricos para estas redes (IBM desarrollo su "*PCRadio*"[7] para utilizarla con ARDIS y otras redes, públicas y privadas).

Estas redes operan en un rango de 800 a 900 MHz. ARDIS ofrece una velocidad de transmisión de 4.8 Kbps. Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta). Las redes públicas de radio como *ARDIS* y *MOBITEX* juegan un papel significativo en el mercado de redes de área local (LAN's) especialmente para corporaciones de gran tamaño. Por ejemplo, elevadores OTIS utiliza *ARDIS* para su organización de servicios.

2.3.2 Redes de área local

[7] La PCRadio es un dispositivo manual con un microprocesador 80C186 que corre DOS, un radio/fax/módem incluido y una ranura para una tarjeta de memoria y 640 Kb de RAM.

Las redes inalámbricas se diferencian de las convencionales principalmente en la “Capa Física” y la “Capa de Enlace de Datos”, según el modelo de referencia OSI.

La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos (donde se relaciona directamente con la MAC y la NIC), se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse.

Los dos métodos para remplazar la capa física en una red inalámbrica con respecto a las cableadas son la transmisión de Radio Frecuencia y la Luz Infrarroja.

2.3.3 Redes infrarrojas

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores/emisores en las ventanas de los edificios.

La transmisión Infrarroja es actualmente una alternativa para las Redes Inalámbricas que esta entrando en desuso por el surgimiento de mejores

alternativas. El principio de la comunicación de datos es una tecnología que se ha estudiado desde los años 70. Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.

El mismo principio se usa para la comunicación de Redes, se utiliza un "*transreceptor*" que envía un haz de Luz Infrarroja, hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "Transreceptor Infrarrojo". Los primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor.

2.3.4 Redes de radio frecuencia

Por el otro lado para las Redes Inalámbricas de Radiofrecuencia, la FCC permitió la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia: 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 MHz. Estas bandas de frecuencia, llamadas bandas ISM,

estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera. Para minimizar la interferencia, las regulaciones de la FCC estipulan que una técnica de señal de transmisión llamada *spread-spectrum modulation*, la cual tiene potencia de transmisión máxima de 1 Watt, deberá ser utilizada en la banda ISM. Esta técnica a sido utilizada en aplicaciones militares. La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía debajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia.

Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente:

La secuencia directa (DSSS): En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.

El salto de frecuencia (FHSS): Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 MHz que son utilizadas por hornos de Microondas.

3. TECNOLOGÍAS Y ESTANDARES DE WLANs (*WIRELESS LAN, LAN INALÁMBRICA)*

3.1 Familia IEEE 802.11x

El primer estándar que surge es el 802.11 (1997), el cual sienta las bases tecnológicas para el resto de la familia. No tuvo relevancia por la baja velocidad binaria ("bitrate") alcanzada, cerca de 2 Mbps, y la carencia de mecanismos de securización de las comunicaciones. Muy poco después se publica el 802.11b, cuya acogida comercial tuve y mantiene un gran éxito. Opera en la banda de los 2,4 GHz y permite alcanzar velocidades binarias teóricas de 11 Mbps mediante el empleo de mecanismos de modulación de canal y protección frente a errores bastante robustos, aunque en la práctica es difícil superar una velocidad de datos efectiva de 7 Mbps. Cuando el canal de transmisión es ruidoso, posee un mecanismo de negociación que reduce la velocidad binaria en escalones predefinidos, aumentando paralelamente la robustez de los mecanismos de protección frente a errores. Para complementar su operación, incorpora un protocolo de seguridad de las comunicaciones, el WEP o Wired Equivalent Privacy (privacidad equivalente a redes cableadas), habida cuenta de la imposibilidad de confinar las emisiones en un medio más protegido como es el cable en el caso de las redes fijas. Desafortunadamente, el pretencioso nombre no se corresponde a la realidad, pues muy poco después de su

publicación se descubrieron importantes defectos que permitían la intrusión en las comunicaciones con escaso esfuerzo y un equipo convencional.

Pese a lo anterior, el éxito fue de tal magnitud que aceleró la liberación de nuevos estándares y reclamó una especial atención por entidades de regulación, que empezaron a valorar la ampliación del espectro para este tipo de usos.

Posteriormente un estándar es publicado por la IEEE, éste fue el 802.11a, el cual tiene la particularidad de operar a una mayor tasa de bits (teóricamente hasta 54 Mbps) mediante unos esquemas de codificación de canal más sofisticados y sobre bandas en los 5 GHz. Su empleo no está tan extendido como el 11b por el menor rango de cobertura debido a la mayor atenuación de las frecuencias empleadas en algunos casos y la necesidad de mecanismos de control de potencia que aun no estaban incluidos y se equiparó.

El 12 de junio del 2003 fue aprobado el estándar 802.11g, que mejora ostensiblemente en varios frentes:

Este mantiene el rango de los 2,4 GHz pero amplia la tasa de bits hasta los 54 Mbps teóricos (en la práctica se obtiene una tasa efectiva menor que la mitad).

Mantiene la compatibilidad con el 11b y propone un protocolo de securización más robusto denominado WPA (Wi-Fi Protected Access).

Dichas mejoras han relanzado más si cabe la confianza del mercado en la tecnología y como consecuencia de ello las implantaciones y venta de productos.

Después de aquellos estándares (a, b y g), la IEEE no dejo de trabajar y posteriormente publicó nuevos estándares y trozos auxiliares de ellos como el 802.11i, que es realmente la formalización del WPA, con funcionalidades restringidas debido a la presión de mercado por encontrar una solución al grave problema de seguridad puesto de relevancia con el antiguo WEP.

Otro estándar importante es el 802.11e, el cual define los mecanismos para proporcionar calidades de servicio bajo las WLAN. Esto dio entrada a aplicaciones que permiten ofrecer servicio de garantía por priorización del tráfico, necesario para usos como la telefonía / voz por IP en estas redes (VoWLAN), televisión, videoconferencia y, por ende, ampliando el potencial de la tecnología.

También es de gran relevancia el 802.11h que permite incluir las nuevas condiciones de utilización que muchos países, exigen para el uso de los rangos de frecuencias en torno a los 5 GHz para redes inalámbricas, como son el

control automático de la potencia emitida, el análisis continuo del espectro para evitar el empleo de canales ya ocupados y la selección dinámica de frecuencias. Con ello se buscó solventar el problema de posibles interferencias de estas redes con las emisiones de satélite y militares que también las emplean y que son prioritarias.

Una de las claves del éxito comercial ha sido la buena interoperabilidad existente entre equipos de diferentes fabricantes, labor que ha llevado a cabo la Wi-Fi Alliance. Este organismo, con cerca de 200 empresas entre sus miembros y 800 productos certificados en el día de hoy, ha fomentado la tecnología y garantizando su genérico buen uso.

Otros estándares muy importantes de la familia IEEE son el 802.11d que se encarga de tratar los múltiples dominios reguladores que serán tratados mas adelante.

En la siguiente tabla se resumirán las principales características de la familia de estándares IEEE 802.11x

Tabla 1. Estándares IEEE 802.11

Estándar	Frecuencia portadora	Velocidad de datos	Resumen
802.11ª	5.1-5.2 GHz 5.2-5.3 GHz 5.7-5.8 GHz	54 Mbps	La potencia máxima es 40 mW en la banda 5.1, 250 mW en la banda 5.7 (USA).
802.11b	2.4-2.485 GHz	11 Mbps	El más popular
802.11d	N/D		Múltiples dominios reguladores
802.11e	N/D	N/D	Calidad de servicio
802.11f	N/D	N/D	Protocolo de conexión entre puntos de acceso (Inter-Acces point Protocol, IAPP).
802.11g	2.4-2.485 GHz	36 o 54 Mbps	
802.11h	N/D	N/D	Selección dinámica de frecuencia (DFS)
802.11i	N/D	N/D	Seguridad

3.2 El estándar 802.11

El estándar 802.11 de IEEE debe ser observado con un grado adicional de detalle debido a que tiene un conjunto de variantes y quizás lo más importante, es que ha capturado la atención de los proveedores principales de esta tecnología y disfruta por un amplio margen la mayor parte del mercado y esto no lo pone a la paria.

El IEEE adoptó el estándar 802.11 en 1997 y se convirtió en el primer estándar WLAN. De acuerdo con la IEEE, 802.11 IEEE principalmente controla las capas

1 y 2 del modelo OSI, las cuales son la capa física y la capa de enlace de datos, respectivamente.

3.2.1 La capa MAC (Control de acceso al medio) 802.11

La capa MAC es un subconjunto de la capa de enlace, que a su vez es adyacente a la capa física en una red basada en IP. Tres funciones de la capa 1 en una red 802.11 son:

Funciona como la interfaz entre la capa MAC en dos o más ubicaciones geográficas. Estas ubicaciones normalmente sólo están a pocos cientos de metros o menos de distancia.

Se encarga de la detección real de los sucesos CSMA/CD, mismos que ocurren dentro de la capa MAC.

Efectúan la modulación y desmodulación de la señal entre dos puntos geográficos en los que residen equipos 802.11. Este esquema de modulación puede ser DSSS o FHSS.

El estándar IEEE 802.11 también define una técnica de cambio de velocidad que permite a las redes reducir las velocidades de datos a medida que ocurren cambios en la distancia, calidad y fuerza de la señal. Las velocidades de datos de 802.11b IEEE pueden ser tan altas como 11 Mbps con modulación DSSS, en tanto que las velocidades de datos moduladas con FHSS pueden ser 1 o 2

Mbps. El estándar también permite la compatibilidad entre los radios 802.11a y 802.11b la parte de una red 802.11a que usa equipos 802.11b dará como resultado velocidades de datos más lentas que las del estándar más viejo.

La capa MAC es una subcapa de la Capa 2 del modelo OSI y controla la conectividad de dos o más puntos a través de un esquema de direcciones. Cada computadora portátil o punto de acceso tiene una dirección MAC. El estándar IEEE 802.11 define la forma en que funcionan las direcciones, además ciertas funciones de la capa 1. Este estándar es parecido en muchos aspectos al estándar Ethernet. De hecho define lo siguiente:

Las funciones que se requieren en un dispositivo compatible con 802.11 para operar en una red de igual a igual o integrado en una WLAN existente

La operación del dispositivo 802.11 dentro del rango de otros dispositivos 802.11 y la forma en que la tarjeta cliente migraría físicamente de un punto de acceso al otro.

Servicio de control de acceso y entrega de datos al nivel MAC para las capas superiores de la pila de protocolos de red.

Varias técnicas de interfaz de señalamiento en la capa física.

Privacidad y seguridad en los datos del usuario que se transfieren a través del medio inalámbrico.

La capa MAC es lo que hace que una WLAN sea diferente de una LAN Ethernet debido a que gracias a esta es posible que los usuarios de la red adquieran movilidad sin necesidad de estar conectados físicamente a una red cableada.

Es por eso que la capa MAC 802.11 está obligada a hacerse cargo de ciertas funciones que normalmente pertenecen a las capas mas altas del modelo OSI, por ejemplo la capa de sesión (capa 5), que controla el inicio y terminación de sesiones. En el estándar MAC 802.11, el flujo de información se realiza mediante un método del mejor esfuerzo, que también se conoce como “sin conexión”. Los enlaces sin conexión son en los que el extremo receptor del enlace no verifica la recepción de los datos con el extremo transmisor. La técnica que utiliza la capa MAC se conoce como Accesos múltiples de sensor de portadora con detección de colisiones (CSMA/CD) que es una técnica que requiere que el transmisor ‘’escuche’’, lo que ocurre en el entorno local, para asegurarse de que no existan otras transmisiones en la frecuencia que tiene asignada. La detección real se efectúa en la capa Física, pero el control del tiempo para las transmisiones se efectúa en la capa MAC. Los radios 802.11 están programados de manera que es aleatorio el tiempo entre los intentos para determinar si un canal de radio en particular esta disponible. Se emplearon algunas estadísticas simples para establecer que la probabilidad más alta que un canal este en uso, es justo después de que un intento de transmisión fue detenido debido a que el canal de radio estaba siendo usado

por otro transmisor. Es por esta razón que el tiempo entre los intentos para transmitir tiene un ritmo aleatorio. La cantidad de tiempo entre la repetición de intentos con frecuencia se conoce como tiempo de retroceso.

Otra función que proporciona una capa MAC 802.11 es la de seguridad, la que normalmente se controla en la capa de presentación (capa 6). La medida de seguridad compatible con este estándar es la Privacidad equivalente al cableado (WEP) que es un método para manejar claves y cifrar los datos. Mas adelante hablaremos más sobre esta función.

La siguiente tabla ilustra las principales diferencias entre los estándares 802.11 (b, g y a).

Tabla 2. Comparación de estándares IEEE 802.11

	802.11b	802.11g	802.11a
Frecuencia	2.4 GHz	2.4 GHz	5.7 GHz
OFDM	No	Sí	Sí
Velocidad de datos	11 Mbps	54 Mbps	54 Mbps
Numero de canales que no se traslapan	3	3	12

3.3 Bluetooth

Aunque BlueTooth en realidad es un estándar WLAN, existe una confusión considerable en cuanto al hecho de que compite o no directamente con 802.11 y HomeRF, o con ambos. En resumen BlueTooth no compite directamente con

802.11 y compite sólo de una manera superficial con HomeRF. La principal razón de esto es que ésta tecnología tiene como propósito ser un estándar con un rango nominal de aproximadamente 1 a 3 metros. Su intención es conectar computadores portátiles con teléfonos celulares, PDA con computadores portátiles y teléfonos celulares, además de otros dispositivos similares. La segunda razón es que está relativamente limitado a la velocidad con aproximadamente 1.5 Mbps; lo que es aproximadamente una décima parte de la velocidad del estándar 802.11 a y 802.11g.

Las primeras versiones de la especificación de ésta tecnología se emitieron a principios de 1999 y se esperaba que la versión 2 fuera lanzada en el 2002 y aun la estamos esperando. Esta demora puede traer problemas al estándar, en especial, debido a que BlueTooth 1 ha estado expuesto a una considerable cobertura por parte de los medios, mismo que fue publicado a mediados de los noventa. En otras palabras, la versión 1 necesito aproximadamente 4 años para que se especificara y se publicara, por lo que un retraso excesivo en la publicación de BlueTooth 2 podría debilitar la base de apoyo, ya que el grupo de apoyo de ingenieros y compañías puede dedicarse a otros estándares que están más próximos a su publicación o ya están en el mercado.

No obstante que en realidad se acerca a la tendencia de los dispositivos que realmente son de banda ancha, de acuerdo con su página web principal, la velocidad de datos máxima es de 1 Mbps y se aclara que es una velocidad de datos aproximada. Se debe esperar que la capacidad de salida real está

alrededor de 750 Kbps, dependiendo de la carga que se use para la administración de la seguridad y el salto de frecuencia.

El estándar BlueTooth tiene dos puntos fuertes:

Tamaño. Este factor le permite conectarse en relojes de mano, PDA y otros dispositivos electrónicos pequeños en los que el tamaño es un criterio de diseño importante.

Ahorro de energía. BlueTooth usa 30 microamperes, lo que es una cantidad muy pequeña de energía. Usa una fracción de la energía que emplea un reloj de mano normal y utiliza órdenes de magnitudes más bajas que las que usan los teléfonos celulares. Esta característica también juego un buen papel en la industria, la cual con frecuencia crea dispositivos, como auriculares inalámbricos, basándose en la cantidad de energía que se requiere de una batería para proporcionar un ciclo de trabajo significativo 8período de operación continua).

En términos de seguridad BlueTooth cuenta con un método de cifrado, pero no se especifica en la página web. Se debe mencionar que un esquema de saltos FHSS de 1600 saltos por segundo, además de un rango muy limitado, de 1 a 3 metros, ocasionará que sea muy difícil interferir la comunicación a distancia.

Para dar algo de referencia sobre ésta tecnología, algunos de los productos basados en BlueTooth se encuentran en el mercado, principalmente en le área

de conexión de teléfonos celulares con PDA, teclados y mouse con PC, cámaras con PC y conexiones similares.

Aquí, en la siguiente figura un pequeño ejemplo de lo que sobre lo que se puede montar sobre la red de Bluetooth:

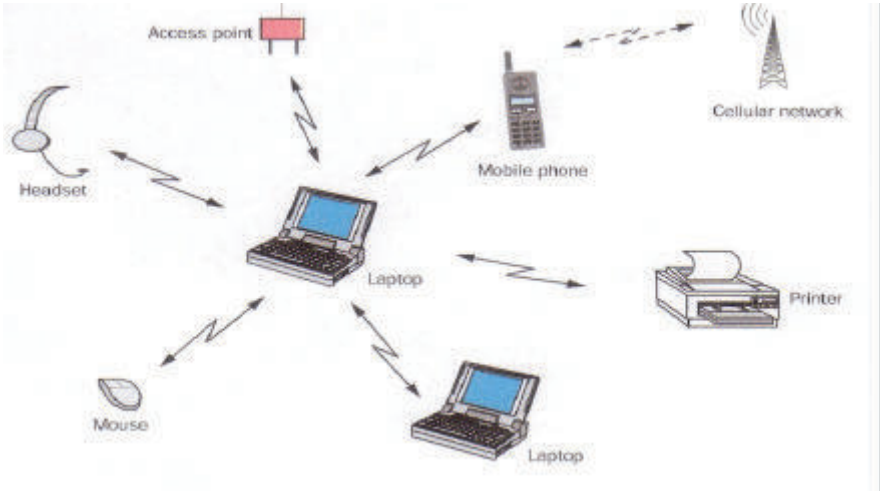

Figura 1. Red Bluetooth

3.4 Hiperlan

Es un estándar definido para las LAN sin cable de alta velocidad, definido por la unión europea en 1992 para operar en la frecuencia de 5.7 GHz. Seis años después, aun no aparecían los primeros productos HiperLan y se suponía un fracaso de la tecnología. A pesar de esto, los Estados Unidos asignaron un espectro para redes de alta velocidad, aunque sin exigir los estándares

HiperLan. Esta banda es la U-NII (Unlicensed National International infraestructure).

3.4.1 HiperLan1

Fue el estándar propuesto por el ETSI (European Telecomunications Standards Institute)[8] en 1992, cuando por primera vez reconoció la necesidad de las Lan sin cable de alta velocidad. Como la familia IEEE 802.11, gran parte de el se basa en Ethernet, aunque su tecnología de acceso por radio fue directamente tomada de GSM. Debido a que GSM a tenido tanto éxito, ETSI a menudo reutiliza algunas partes de el en estándares nuevos aparentemente no relacionados. La velocidad máxima se supone que es 23.5 Mbps, pero nadie sabe a ciencia cierta la que podría alcanzar, debido a que existe muy poco equipamiento HiperLan1.

3.4.2 HiperLan2

Utiliza el mismo espectro que HiperLan1 pero, por otro lado, esta mucho más cercano a IEEE 802.11a. Tiene la misma velocidad de datos máxima de 54 Mbps, utilizando la misma tecnología coded OFDM (Orthogonal Frequency

[8] Principal órgano Europeo de estándares, entre cuyos proyectos están incluidos GSM, UMTS, DECT.

División Multiplex)[9]. En cierto momento, hubo planes para unir HiperLan2 y IEEE 802.11a. en un solo estándar pero actualmente parece improbable.

3.5 HomeRF

Como su nombre lo indica está diseñado para las redes domésticas, se basa en la versión original FHSS (Frequency Hopping Spread Spectrum) de 802.11 y fue diseñado principalmente para facturación, más que para alcanzar velocidad; opera en la banda ISM (Industrial, Scientific and Medical) de 2.4 GHz. Su única innovación importante es que soporta la telefonía lo que podría presentar una ventaja importante en el mercado doméstico. El resto de estándares esta diseñado para datos solamente y necesita software adicional para voz. El estándar también se conoce con el nombre de SWAP (Shared Wireless Access Protocol), por que lo comparten distintos tipos de tráfico.

HomeRF soporta hasta 127 equipos conectados (teléfonos, hornos, video caseteras, PC's, etc.). Tiene topología Ad Hoc o vía infraestructura con un equipo central de Acceso. Transmite a 10 Mbps, hasta 45 metros.

[9] Es un sistema que divide una corriente de datos de alta capacidad en múltiples corrientes de menor capacidad y las envía por separado

4. REDES WI-FI (IEEE 802.11b)

4.1 Topologías de red

Las redes 802.11 tienen dos topologías distintas, la topología ad-hoc y la topología de infraestructura.

Dentro de cada una de estas topologías existe el conjunto de servicio básico (Basic Service Set, BSS), que consiste de dos o más nodos, a veces conocidos como estaciones. Un nodo o estación es una plataforma individual, como un AP o una tarjeta interfaz de cliente (por ejemplo, una tarjeta PCMCIA o mini-PCMCIA). Un BSS tiene dispositivos que se reconocen y trabajan en conjunto unos con otros para minimizar la cantidad de colisiones que existen dentro del dominio BSS.

Las redes ad-hoc, normalmente están compuestas de dos o más clientes que son iguales entre ellos, por ejemplo, computadoras portátiles o PDA's con tarjetas 802.11 integradas. La figura 2 ilustra una red ad-hoc.

Figura 2. Red ad-hoc

Una red ad-hoc se clasifica como un conjunto de servicio básico independiente (IBSS), en donde no existe un punto de acceso dentro de este conjunto de servicio. Las funciones de coordinación son asumidas de forma aleatoria por una de las estaciones presentes. El trafico de información se lleva a cabo directamente entre los dos equipos implicados sin tener que recurrir a una jerarquía superior centralizadora, obteniéndose un aprovechamiento máximo del canal de comunicaciones. La cobertura se determina por la distancia máxima entre dos equipos la cual suele ser apreciablemente inferior a los modos en los que hay punto de acceso. Es un modo de empleo infrecuente por las connotaciones de aislamiento que conlleva. Es útil cuando el trafico solo fluye entre los equipos presentes en su cobertura.

El conjunto de servicio que es por un gran margen más común dentro del mundo 802.11, es el modo de red infraestructura. A medida que los que se encuentran dentro de computadoras portátiles, por ejemplo, las tarjetas

PCMCIA, tienden a ser bastante portátiles (o nómadas), los AP tienden a ser relativamente estáticos y uno o más proporcionan conectividad extensa con la red. El AP en este caso se considera la extensión base con la que se conectan todos los clientes y en general es el dispositivo que controla el trafico que fluye entre el AP y los distintos clientes; En otras palabras, existe poco o nada de comunicación de cliente a cliente. La figura 3 ilustra un ejemplo de esta red de infraestructura que a la vez es un IBSS.

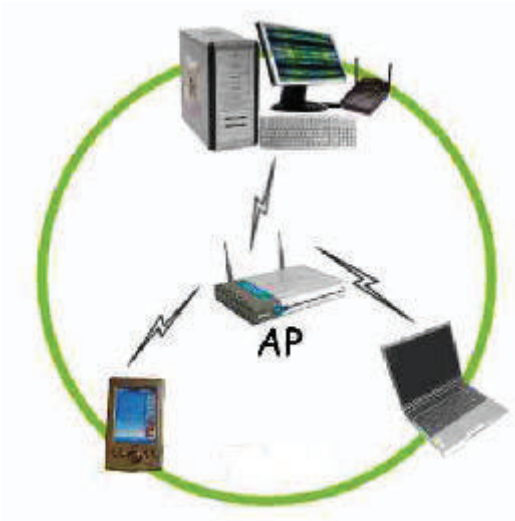

Figura 3. Red Infraestructura IBSS

La referencia apropiada para los clientes y AP en una red infraestructura es Conjunto de servicio extendido (Extended Service Set, ESS), debido a que este termino incluye dispositivos que provienen de mas de un BSS y normalmente esta conectada a Ethernet a través de su sistema de distribución (DS), como una LAN, a lo largo de toda una empresa. Cuando el sistema de distribución es inalámbrico se denomina WDS. Una ilustración de lo anterior lo vemos en la figura 4.

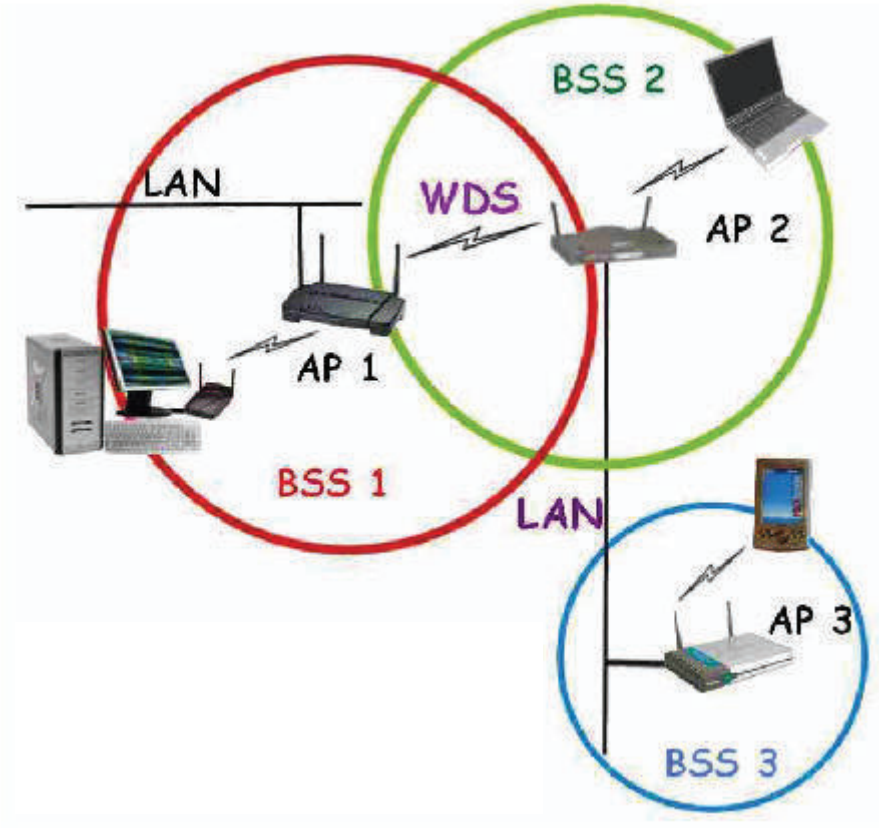

Figura 4. Red infraestructura ESS

4.2 La capa física en las redes Wi-Fi

Considerando el modelo OSI para la estructura en capas de una red Ethernet inalámbrica, la capa física es la de nivel inferior que nos proporciona los mecanismos para transmitir la información por un determinado medio físico, en este caso el medio aéreo. Esto comprende la modulación específica para el canal de transmisión, los mecanismos de protección de la información frente a ruido e interferencias y la estructuración en canales de uso.

Uno de los aspectos novedosos de la tecnología es el empleo de una técnica denominada de espectro ampliado en virtud de la cual se dispersa la energía necesaria para emitir un mensaje, tal y como refleja la figura 5.

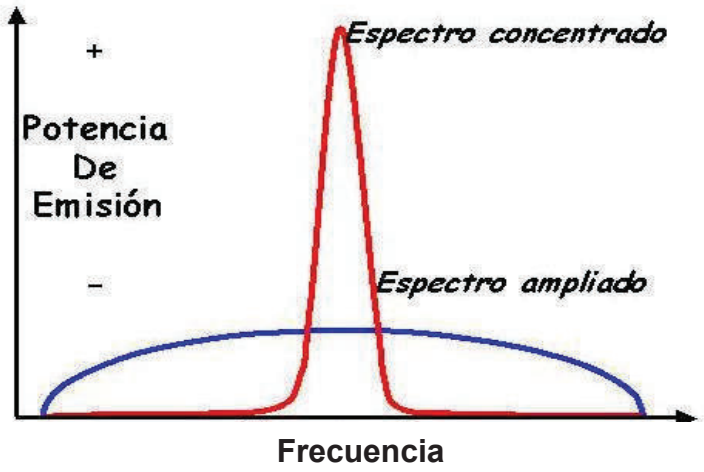

Figura 5. Técnica del espectro ampliado

La ventaja que ofrece es que frente a interferencias y ruido concentrados en una banda estrecha, la información enviada no sufre alteración.

Para obtener esta ampliación del espectro se recurre a redundar la información original.

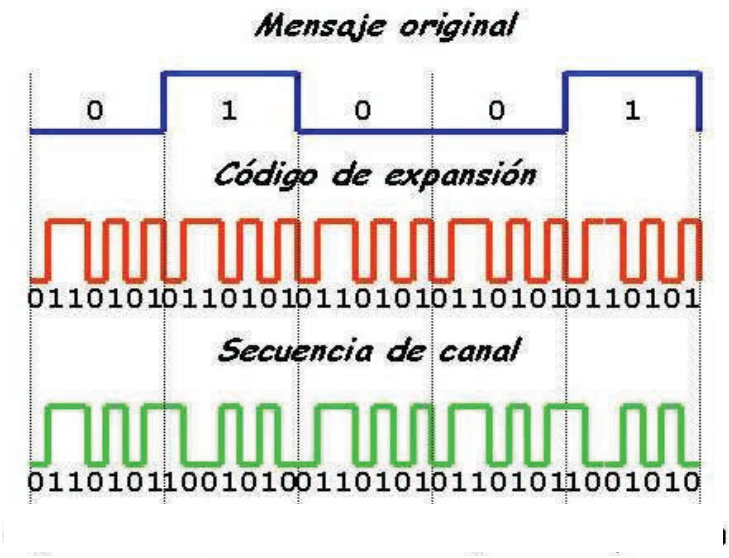

Figura 6. Mecanismo del código de expansión

En el ejemplo de la figura 6, se observa como cada bit del mensaje a transmitir se expande mediante un código de n bits (7 u 11) denominado código de expansión o chipping code. De esta forma el mensaje de salida es n veces mayor que el original.

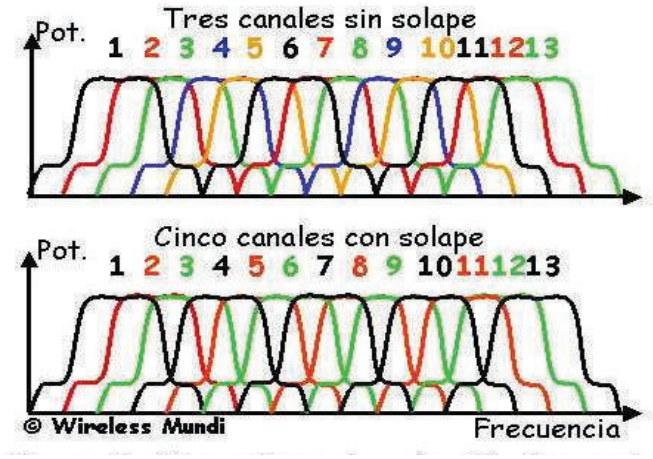

Figura 7. Alternativas de selección de canales

La modulación resultante mediante la combinación de ambas técnicas, denominada DSSS[10], se procede a emitir la secuencia por uno de los 13 canales de 22 MHz con solape parcial entre ellos, tal y como se aprecia en la figura 7.

Si se dispone de una única celda en la zona de cobertura, se puede elegir cualquiera de los existentes. Pero si son más de una las celdas que parcial o totalmente comparten un mismo espacio físico, entonces se deben elegir canales que no presenten solape, pues en caso contrario se producirán interferencias. También en la figura se pone en relevancia que con la estructura de segmentación del espectro disponible sólo es posible disponer de tres canales sin solape y un máximo de cinco con un solape escaso que no producirá excesivas interferencias.

Una vez obtenida la secuencia de canal, se introduce en un sistema de modulación de alta eficiencia y robustez. Dependiendo de la velocidad deseada, el nivel de protección frente a ruidos y el protocolo empleado (b, g, a), se disponen de diversos sistemas: Barker, CCK, PBCC (para 11b) y OFDM (adicional en IEEE 11g y 11a).

La especificación 802.11 permite técnicas de modulación menos complejas, como la modulación de fase por desplazamiento binario (BPSK), la que se usa

[10] Técnica de propagación denominada Espectro Extendido de Secuencia Directa

con un cambio de fase por cada bit modulado para asegurar la obtención del rango máximo; esta velocidad estaría limitada a cerca de 1 Mbps.

La técnica de modulación más compleja siguiente es la modulación por desplazamiento en cuadratura (QPSK), que codifica dos bits de la información en la misma cantidad de espectro que BPSK, aunque obviamente tiene un rango menor.

Ora técnica de modulación compleja es la que usa 802.11b se conoce como modulación de código complementario (CCK). CCK no usa el código Barker[11]; en lugar de eso se basa en una serie de códigos denominados secuencias complementarias. Se pueden usar 64 códigos únicos para codificar los bits individuales en un flujo de datos. En otras palabras, es posible codificar hasta seis bits del flujo de datos, a diferencia del uno sencillo o cero que se usa en el esquema Barker. Luego, el código CCK es modulado con QPSK en radios de 2 Mbps a 11Mbps. Después se envían ocho bits por símbolo (onda senoidal), pero cada uno de los símbolos codifica ocho bits debido a la modulación QPSK, los cuales a su vez se propagan a través de varios canales por medio de la técnica de propagación DSSS. Esto da como resultado 11 mega bits por tiempos de un segundo de 1 MHz del espectro, lo que significa que los radios usaran 22 MHz del espectro. Ahora bien, debido a que aun así es difícil

[11] Flujo de unos y ceros que forman el tráfico y convierten a cada uno de los números individuales en un conjunto de 11 números o fragmentos, también se conoce como secuencia de fragmentación. En otras palabras, cada grupo de 11 bits representa en realidad un solo bit de flujo de datos. Después los fragmentos (11bits) son modulados y se envian a través de uno de los canales sin traslape hacia un cliente.

discernir cual de los 64 códigos únicos se están transmitiendo cuando el rango se agrega, o cualquier elemento degrada la calidad del enlace, se puede observar que es prudente el uso de mas de una modulación o técnica de fragmentación para asegurar que el enlace continúe disponible.

4.3 La capa de acceso al medio

Una vez resuelto el problema del empaquetamiento y modulación de la información, es necesario determinar cómo los dispositivos tienen acceso al medio de transmisión para enviarla y recibirla. Es fundamental considerar que el medio es abierto, en el sentido que pueden coexistir múltiples emisores y receptores en el mismo espacio físico, por lo que es vital el implantar un mecanismo robusto y eficiente de diálogo.

La solución llegó por la modificación del muy conocido protocolo de acceso al medio desarrollado para las redes Ethernet cableadas, el IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD). El nuevo protocolo, CSMA/CA (Collision Avoidance), impone a una estación que desee transmitir que previamente escuche el medio para detectar si otro emisor está realizando esta función. Si es así, esperará un tiempo aleatorio para sondear de nuevo el medio. Cuando detecte que el medio está libre, emitirá una solicitud de ocupación que será escuchada por el sistema que gestione los permisos (el punto de acceso). Si se le concede el acceso, podrá realizar la emisión. De

esta forma también se evita un conocido problema denominado del “nodo oculto”, donde dos nodos dentro de una celda gobernada por un punto de acceso tienen cobertura suficiente para acceder a él, pero están entre sí lo suficientemente alejados para no detectar sus respectivas peticiones (mecanismo RTS/CTS).

Pese a la gran complejidad de los protocolos y su variedad (en alguno casos debida a la conciliación de posturas entre fabricantes participantes en los consorcios de estandarización con propuestas diferentes), ya existen en el mercado sistemas compuestos por tan sólo uno o dos integrados y que realizan todas las funcionalidades de los estándares a, b y g, además de la compleja lógica de seguridad WPA y otras funciones.

Para ayudar a clarificar lo que hace la capa MAC, y para resumir las funciones esenciales de esta capa, en este momento consideraremos las funciones esenciales de esta capa, las funciones principales son:

- Exploración
- Autenticación
- Asociación
- Seguridad
- RTS/CTS
- Modo de ahorro de energía
- Fragmentación

4.3.1 Exploración

Existen dos tipos de exploración dentro del protocolo 802.11, activa y pasiva. En este contexto, ‘’exploración’’ se refiere a los clientes, por ejemplo, tarjetas PCMCIA y dispositivos parecidos, que buscan AP y puentes para grupos de trabajo, por mencionar algunos. La exploración pasiva es obligatoria dentro del protocolo 802.11 y se realiza cuando los clientes exploran cada uno de los canales disponibles. Esta exploración se efectúa con el fin de encontrar una señal AP (Acces Point, en ingles Punto de Acceso) óptima. Este tipo de exploración es muy importante en las instalaciones 802.11, debido a que la mayoría de estas tienen canales traslapados para la cobertura de un área, con el fin de asegurar los niveles de desempeño más altos y una cobertura total. Las señales denominadas beacons (radioeléctricas) se emiten periódicamente por los AP, y las tarjetas las reciben mientras hacen la exploración. Las beacons incluyen a los identificadores de establecimiento de servicio (SSID)[12] y otra información relevante.

Posteriormente, el cliente se conecta con el AP a través de la señal más favorable. El propósito principal de la exploración es asegurar que el cliente se asocie con el AP más adecuado dentro del área.

La exploración activa es un protocolo opcional dentro de 802.11 y en esencia el mismo proceso que una exploración pasiva, la única diferencia es que el cliente

[12] El SSID es una contraseña asignada y distribuida por el administrador de red, que los AP reconocerán después de recibirlas desde los clientes.

envía una trama de prueba y todos los AP dentro del rango responden con una respuesta de prueba. La diferencia operativa entre la exploración pasiva y activa es que cuando un cliente explora de manera activa, no espera las señales radioeléctricas programadas regularmente que envían los AP; En otras palabras, los AP responden de acuerdo con la recepción de la exploración activa. A pesar de que la exploración activa puede ofrecer una pequeña ventaja en términos del tiempo necesario para identificar el AP optimo con el que se puede conectar, también requiere de una carga de trabajo adicional debido a las tramas de transmisiones de prueba recurrentes y las respuestas correspondientes.

4.3.2 Autenticación

La autenticación es el proceso mediante el cual los clientes previamente aprobados pueden integrarse en el dominio de colisión. La autenticación ocurre antes de la asociación, debido a que es durante el proceso de asociación en el que las direcciones IP son reveladas por el AP y asignadas al cliente. La retención de esta información es muy importante para prevenir la falsificación de direcciones, un termino de seguridad que se refiere a la emulación de un cliente o AP autorizado en la WLAN. Existen dos tipos de autenticación dentro del protocolo 802.11:

Autenticación de sistema abierto: Obligatoria dentro de la especificación 802.11. Se realiza cuando el cliente envía una solicitud de autenticación con un SSID a un AP, el cual a su vez responde con la autorización o desaprobación de la autenticación.

Autenticación de clave compartida: Se fundamenta en el protocolo WEP, que se reconoce ampliamente como un protocolo de seguridad ineficaz para cualquier tipo de WLAN, pero en particular en aquellas que usan las redes de empresas pequeñas y medianas, en comparación con las WLAN que se usan en compañías y universidades grandes y campus universitarios.

4.3.3 Asociación

Después de que se ha realizado el proceso de autenticación, la tarjeta del cliente (por ejemplo una PCMCIA) inicia una asociación cuando envía una trama de solicitud de asociación que contiene un SSID y las velocidades de datos soportadas. EL AP responde mediante una trama de respuesta de asociación que contiene un ID (Identificación) de asociación junto con otra información relacionada con el AP especifico, por ejemplo una dirección IP. Cuando el cliente y el AP se han asociado, comienza el proceso de autenticación.

4.3.4 Seguridad

Como se enfatizó antes, el cliente cifra el cuerpo, pero no el encabezado de la trama, antes de la transmisión usando una clave WEP. El AP descifra la trama cuando la recibe usando la misma clave.

Una revisión resumida de la manera en que funciona WEP es que un cliente envía una solicitud de autenticación a un AP, pero en lugar de que el AP responda con una aprobación o desaprobación como en el caso de autenticación abierta, responde mediante el envío de un texto de interrogación dentro del cuerpo de la trama que usa para responder. El texto de interrogación en realidad no es nada mas que un texto que esta cifrado con el propósito de determinar si el cliente tiene o no la clave apropiada para descifrar el texto. Al recibirlo, el cliente usa su clave WEP correspondiente para descifrar el texto y luego vuelve a enviarlo hacia el AP. Al recibir este texto de interrogación, el AP lo descifra y compara con el texto que se envío originalmente al cliente en respuesta a la solicitud inicial de autenticación del cliente. Cuando el texto de interrogación recibido por el AP coincide correctamente, le envía al cliente una trama de autenticación seguido por la información de direcciones IP necesarias del AP y la dirección IP asignada al cliente para esa sesión en particular.

4.3.5 RTS/CTS

RTS/CTS significa Solicitud de envio/Listo para enviar. No obstante que el nombre indica lo que ocurre en esta parte de la capa MAC, lo que no se conoce

muy bien acerca de RTS/CTS es que los usuarios cliente pueden establecer el tamaño máximo de la longitud de la trama que se usará en este protocolo dentro del dominio de colisión. Por ejemplo, cuando el usuario establece la longitud máxima de trama en 1000 bytes, el cliente usara RTS/CTS en todas las tramas que tengan 1000 bytes o más.

Como mencionamos antes este protocolo es muy útil cuando existen nodos ocultos, es decir, dos o más clientes que no se detectan entre ellos debido a que están fuera de sus rangos respectivos. El concepto de un nodo oculto no se debe confundir con la incapacidad de un AP para detectar un cliente. Un AP debe contar con un cliente en un estado asociativo antes de comenzar el intercambio de trafico entre el AP y el cliente.

RTS/CTS elimina los problemas potenciales en el tiempo de las transmisiones entre los clientes que no pueden interactuar mediante RF (frecuencias de radio). Lo que sucede específicamente con los clientes del protocolo RTS/CTS es que el cliente envía una trama RTS a un AP antes de la transmisión de un paquete cuando ocurre un exceso en el tiempo predeterminado. Luego, el AP controlará el tiempo de transmisión al enviar un paquete CTS al cliente que espera la transmisión. Cuan el cliente recibe un paquete CTS incluirá un valor de duración en el encabezado de la trama que evita que el AP reciba paquetes de cualquier otro cliente del dominio de colisión o célula de cobertura. El protocolo RTS/CTS continua funcionando mientras un cliente envíe paquetes

más grandes del tamaño previamente establecido para el fin antes descrito. Es importante observar que cada cliente puede tener tamaño de paquetes únicos, aunque el limite superior para el estándar es de 2312 bytes.

4.3.6 Modo de ahorro de energía

Otra opción disponible a nivel de capa MAC es la reducción del uso de energía, factor muy importante cuando los usuarios tienen clientes, por ejemplo, tarjetas PCMCIA en computadoras portátiles. Cuando esta activado el modo de ahorro de energía, el cliente envía un mensaje al AP indicando que se ira a ‘’dormir’’, lo que se realiza por medio del bit de estado localizado en el encabezado de cada trama que se envía desde el cliente. Al recibir la solicitud de ir a dormir, enseguida el AP coloca en el búfer los paquetes correspondientes al cliente.

El modo de uso de energía predeterminado para los clientes es el Modo siempre activo (Constant Awake Mode, CAM), donde el cliente permanece constantemente en un modo de estado activo. Pero si el usuario lo desea, puede utilizar un modo de energía mas bajo, denominado Modo de acceso de sondeo (Polled Acces Mode, PAM). Sin embargo incluso cuando esta en el modo de dormir, el cliente debe activarse en forma periódica para recibir desde el AP un paquete llamado Mapa de información de trafico (Traffic Information Map, TIM), el cual es una notificación al cliente de que existe trafico esperando

en el AP. Cuando el trafico haya sido transferido desde el AP hacia el cliente, este regresara a dormir.

4.3.7 Fragmentación

En el contexto del estándar 802.11 este concepto se refiere a la capacidad de un AP para dividir paquetes en tramas más pequeñas. Con frecuencia, esto se hace de modo que la interferencia RF sólo elimine a los paquetes más pequeños. Recuerde que un dispositivo debe enviar un paquete ACK al dispositivo transmisor para confirmar que ha recibido el paquete exitosamente. Tiene sentido que algunos paquetes tengan que ser retransmitidos. En estos casos, mientras más pequeña sea la transmisión, será mejor el desempeño general dentro de un dominio de colisión, debido a que los otros clientes no tendrán que esperar hasta que la retransmisión se haya completado. La fragmentación también permite el incremento de las cantidades de tiempo libre en el canal. Al igual que el protocolo RTS/CTS, el estándar 802.11 permite al usuario establecer el umbral del tamaño de la trama máximo antes de que la plataforma fragmente el paquete. Cuando el usuario ha establecido sus umbrales de fragmentación, ninguna trama será más grande del tamaño máximo permitido que estableció el usuario.

Además de evitar las colisiones y perdidas de la señal, la capa MAC es responsable de las direcciones fuente y de destino del paquete que se envía,

además del CRC. Cada nodo en una red 802.11 es identificado mediante su dirección MAC y usa un esquema de direccionamiento que es idéntico al de Ethernet, el cual es un valor de 6 bytes-48 bits.

4.3.8 Roaming 802.11

Se denomina roaming a la posibilidad por parte de una estación inalámbrica (y por su naturaleza habitualmente móvil) de desplazarse fuera de la cobertura de su celda y conectarse a otra manteniendo la continuidad de las aplicaciones que anteriormente ejecutaba.

El punto de partida lo tenemos en una estación autentificada en varios BSS y asociada a uno de ellos. A medida que se desplaza comenzará a perder nivel de señal por lo que a partir del momento que su valor decaiga por debajo de cierto umbral, la estación procederá automáticamente a una búsqueda de alternativas

El primer proceso que se establece es el análisis de diversos canales de emisión posibles en busca de alternativas, proceso denominado sep. Dentro de un canal determinado procede a la evaluación de las estaciones presentes como alternativa de conexión, denominado scanning o la exploración tema que fue tratado anteriormente. Se evaluará el nivel de la señal y se obtendrá el SSID de la nueva celda. Obviamente la primera condición para que se pueda producir el roaming es que nos encontremos en un sistema ESS (ambas celdas

estén comunicadas por un sistema de distribución) y que las identificaciones SSID sean idénticas.

Una vez realizado el sweep entre canales y el scanning en cada uno, la estación ya puede tomar la decisión de a que AP se conecta. En primer lugar recupera los paquetes de información que pudiesen haber llegado a la antigua celda e inmediatamente solicita la re-asociación a la nueva. En múltiples casos, y debido a la inmadurez del protocolo de conexión entre puntos de acceso (Inter-Acces Point Protocol, IAPP) es necesario realizar de nuevo la autentificación. Finalmente el nuevo AP comunica al antiguo la suscripción de la estación para que elimine los datos sobre la misma. Todo este proceso puede llevarse a cabo cuando ambas celdas poseen un rango de direccionamiento IP en la misma subred de tal forma que el equipo mantiene la dirección IP y no se produce interrupción de las sesiones en curso, lo cual implica que están interconectados a través de bridges (puentes de nivel 2). Si los rangos son diferentes y se atraviesan routers (conectividad a nivel 3), este mecanismo no es valido y se requieren otras opciones como el establecimiento de redes privadas virtuales (VPN's) o nuevos mecanismos todavía en desarrollo como Ip móvil

Antes de continuar adentrándonos en aspectos más puntuales de las redes 802.11 es preciso conocer algunos equipos muy importantes a considerar en el diseño de una WLAN.

5. EQUIPOS PARA INFRAESTRUCTURA

Se enumeran a continuación los principales tipos de equipos empleados para la construcción de infraestructuras de redes inalámbricas y que serán empleados por los equipos terminales de cliente para la apropiada interconexión.

Aunque se clasificaran de una manera formal, en la realidad los equipos de los fabricantes suelen integrar modos híbridos de funcionamiento que diluyen dicha estructuración. Por ejemplo es ya normal encontrar gateways que operan además como puntos de acceso y bridges, o bridges como APs y repeaters. Además de esta clasificación, en casi todos los casos existen modelos de interior, pensados para operar en recintos cerrados y protegidos, y de exteriores, más robustos y con mayor margen de temperaturas de funcionamiento. Conozcamos ahora con más detalle los elementos clave de una red inalámbrica.

5.1 Punto de acceso ("*Access Point*", AP)

Aunque a lo largo de las paginas anteriores hemos venido tratándolo, es preciso formalizar un concepto de este componente importantísimo de las redes 802.11. Es un nodo especial en una red inalámbrica que actúa como punto centralizador y gestor del tráfico del resto de equipos (terminales de cliente) subscritos a él y dentro de la celda de cobertura (ver Figura 8).

Figura 8. Configuración básica de un punto de acceso

Dispone comúnmente de una interfaz ethernet que le permite estar interconectado a una red cableada (LAN), además de la interfaz inalámbrica por la cual se conectan los equipos de dicha naturaleza. Permite la comunicación entre ambas interfaces y entre los propios equipos inalámbricos a nivel 2 (modelo OSI). En general en una misma localización puede coexistir más de un punto de acceso siempre que no interfieran fuertemente sus frecuencias de funcionamiento. Los equipos presentes estarán subscritos sólo a uno.

Esta definición de punto de acceso es muy genérica de tal forma que otros equipos inalámbricos como routers y bridges realmente se pueden considerar como APs. Sin embargo los fabricantes mantienen esta definición para catalogar los equipos más genéricos y elementales, aunque funcionalmente en

realidad se pueden equiparar a bridges que unen un segmento de red cableada y otro (de alguna forma virtual o no cableado) inalámbrico.

La configuración de estos equipos es muy sencilla, apenas necesitando la introducción de su dirección IP (en la mayoría de ellos se puede activar el cliente DHCP que poseen y de esta forma la capturan automáticamente), la del gateway por defecto, los parámetros de la parte inalámbrica y su securización.

5.2 Puentes (Bridges)

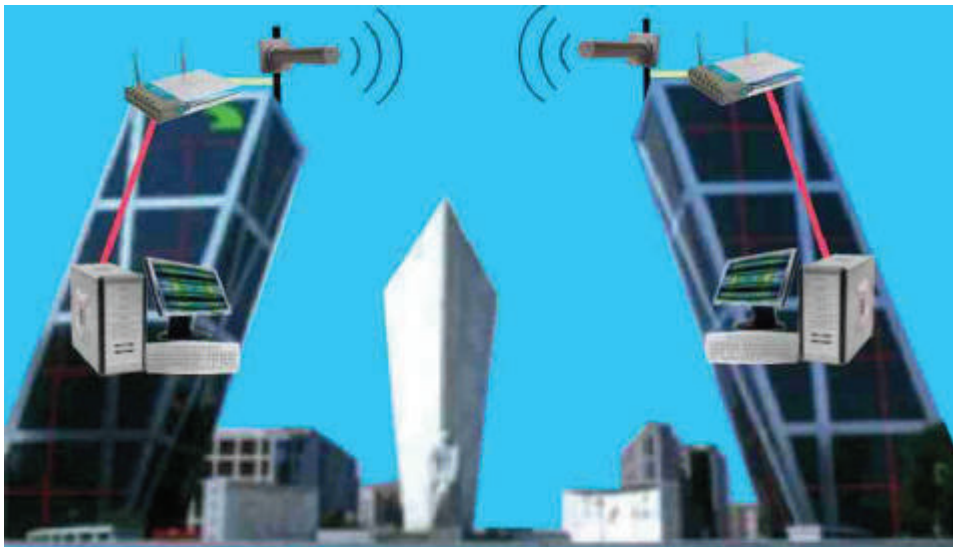

Figura 9. Enlace punto apunto mediante bridges o puentes

Son elementos que interconectan dos o más redes locales (a nivel 2 OSI). En el mundo wireless el concepto se matiza: deben interconectar redes locales fijas (ver Figura 9). Esta definición expone su principal uso, la interconexión de

rede fijas separadas por una distancia física la cual se ha cubierto mediante un segmento inalámbrico. Poseen dos interfaces, uno ethernet y otro inalámbrico. En cada red fija se ubica un bridge inalámbrico, orientando las antenas de ambos equipos para la mejor recepción. En caso de redes en edificios distantes, se suelen instalar antenas directivas de alta ganancia en los tejados lo que permite cubrir distancias en visión directa de hasta unos pocos kilómetros. Los parámetros inalámbricos (canal de frecuencia, bitrate, identificador de servicio-SSID, etc.) de ambos extremos deben ser idénticos para posibilitar la comunicación. Virtualmente se pueden encadenar un número ilimitado de parejas de bridges para enlazar infraestructuras muy distantes o con obstáculos entre sí.

La configuración de estos dispositivos suele ser también bastante simple, requiriendo adicionalmente a los parámetros indicados para un AP poco más que la introducción de la dirección IP del bridge del otro extremo.

Los bridges que se encuentran comercialmente disponibles suelen agregar otras funcionalidades como son el disponer de otros modos de operación: como AP, repeater e incluso como adaptador de red para equipos de cliente.

5.3 Repetidores

Permiten extender la cobertura de APs mediante la regeneración y re-envío de información a zonas anteriormente sin suficiente señal (ver Figura 10).

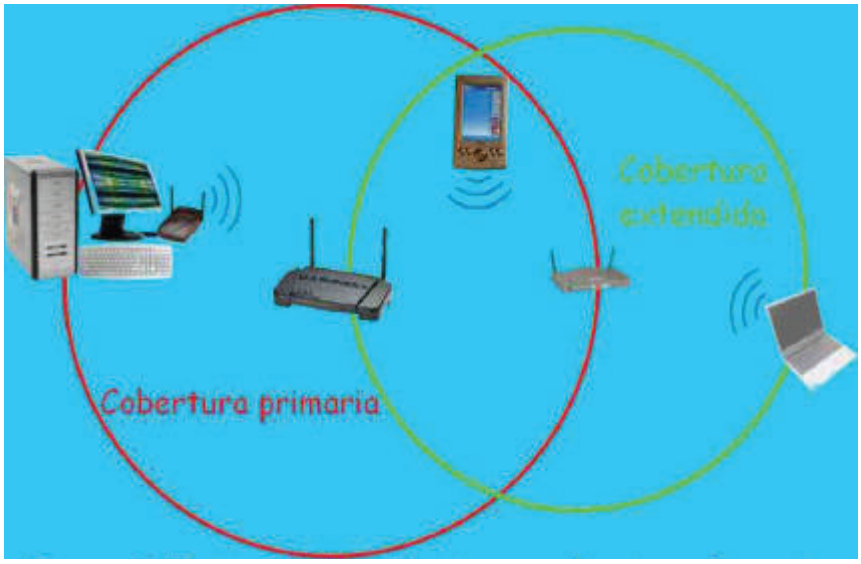

Figura 10. Extensión de cobertura mediante un repetidor

Poseen un único interfaz inalámbrico, que les permite conectarse por un lado al punto de acceso para el cual operan, y por otro lado a los equipos inalámbricos que se le subscriben. Operan con los mismos parámetros que el AP para el cual trabajan (frecuencia, bitrate, etc.). La ventaja de extender de esta forma la cobertura de las redes tiene su precio; dado que toda la información que un equipo le transmite la tiene que remitir al AP, la eficiencia de la solución es inferior al 50%. También es factible encadenar numerosos repetidores para

ampliar todavía más el alcance, pero numerosos problemas que aparecen por colisiones, retardos de señal y penalización en el uso del espectro, no aconsejan emplear más de uno.

En el mercado apenas existen como tal estos equipos. Dependiendo del fabricante, muchos gateways como Aps y bridges pueden configurarse en modo de funcionamiento repeater, siendo la solución empleada.

5.4 ROUTERS Y GATEWAYS

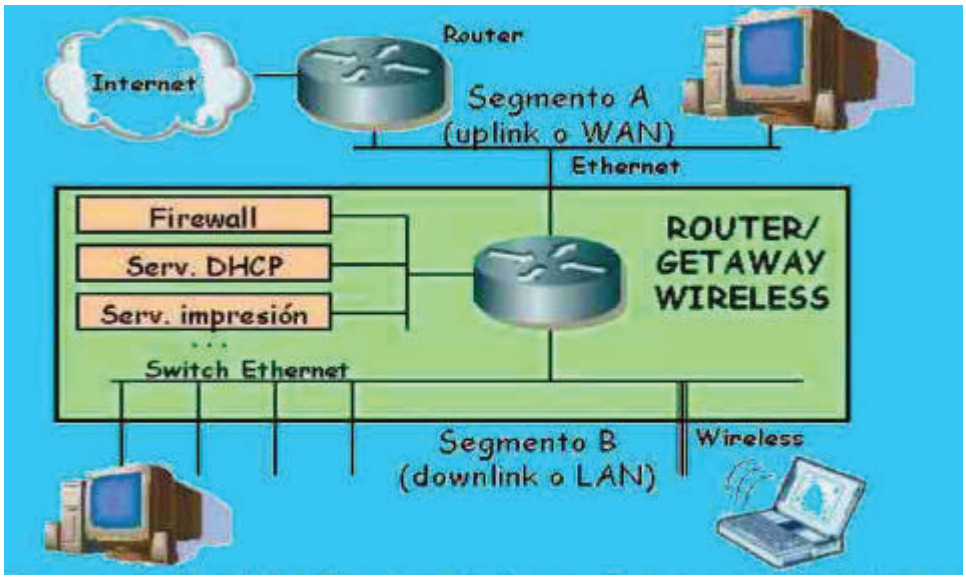

Figura 11. Modelo funcional de un gateway inalámbrico

Poseen capacidad de enrutamiento (niveles 3 y 4 OSI) de los paquetes de información que los atraviesan. Una de sus interfaces es inalámbrica,

existiendo al menos otra fija ethernet a la cual se suele denominar puerto WAN (ver Figura 11).

La mayoría de modelos existentes en el mercado no posee funcionalidades puras de router, sino que están especialmente diseñados para actuar como pasarela entre la red inalámbrica directamente gestionada por el equipo (genéricamente llamada LAN) y las redes externas (red local de empresa, red de acceso a Internet u otras). Por ello con frecuencia se les denomina gateway (pasarela).

Su complejidad interna es superior al resto de los otros equipos. No sólo realizan labores de mayor procesamiento de la información como el enrutamiento, sino que además han sido enriquecidos con funcionalidades avanzadas en networking (traducción de direcciones de red y de puerto por NAT y PAT respectivamente o servidor DHCP de direccionamiento propio) y seguridad (firewall interno avanzado, listas de acceso por dirección MAC ethernet, bloqueo de acceso a urls para control paterno, restricción de uso por franja horaria).

Además de lo anterior, suelen proporcionar en la parte LAN, además del interfaz wireless, un conmutador ethernet integrado de varios puertos. Ya menos frecuente, también algunos modelos poseen un servidor interno de impresión junto a un puerto serie, paralelo o USB para conectar una impresora.

Igualmente existen modelos que poseen un interfaz para interconectarse directamente con redes ADSL.

Aunque por el momento raramente presentes, pronto se extenderá la gestión de redes privadas virtuales (VPNs) e incluso proporcionar voz sobre IP (VoIP).
De forma análoga al resto de los equipos, los gateways pueden proporcionar modos de configuración que les permiten operar como puntos de acceso, repeaters e incluso bridges.

Con toda esta riqueza de funciones, los gateways reúnen en un único equipo las prestaciones que hasta el momento necesitaban varios (un router, un AP wireless, un módem ADSL, un firewall, etc.) y a un precio muy competitivo.

6. CONSIDERACIONES DE FUNCIONAMIENTO OPTIMO DE UNA WLAN BASADA EN EL ESTÁNDAR 802.11B

Wi-Fi es un nombre comercial desarrollado por un grupo de comercio industrial llamado Wi-fi Alliance (Alianza Wi-Fi), cuyos estatutos detallaremos posteriormente.

Wi-Fi describe los productos de WLAN's basados en los estándares 802.11 IEEE y se diseñó para que tenga un nombre más accesible para los usuarios, de la misma manera que Ethernet y Token Ring son más fáciles de aprender que 802.3 y 802.5 IEEE, respectivamente. En principio, Wi-Fi fue creado para describir solo los dispositivos con velocidades máximas de 11 Mbps que operaban en la porción de 2.4 GHz del espectro de frecuencia y que cumplían con la especificación 802.11b IEEE. Mas tarde se decidió que Wi-Fi debería ser extendido para incluir los productos con velocidades de datos máximas de 54 Mbps que operan en las porciones de 2.4 GHz y 5 GHz del espectro de frecuencia y que están basados en las especificaciones 802.11g y 802.11a de la IEEE. A lo largo de este capitulo Wi-Fi se refiere sólo a los productos compatibles con el estándar 802.11b IEEE.

Para garantizar el funcionamiento optimo de una red Wi-Fi es necesario medir el desempeño de esta red en función de los siguientes parámetros:

- Velocidades de datos
- Capacidad de salida
- Alcance en distancia: Rango
- Interoperabilidad

6.1 Velocidades de datos que soporta Wi-Fi

Aunque la promoción del estándar se hace para 11 Mbps, el estándar 802.11b se diseño para que en realidad opere a velocidades de datos de: 1, 2, 5.5 y 11 Mbps. Velocidades que están disponibles en el mismo medio físico, en una porción de casi 80 MHz del espectro de frecuencia, iniciando de 2.4 GHz, que luego se divide entre 11 y 14 canales, dependiendo de las especificaciones gubernamentales.

La forma en que estas velocidades pueden variar no es función de incrementar o disminuir el tamaño de la capa física o cambiar la cantidad de ancho de banda, si no que, por el contrario, es una función del tipo de modulación que se emplee.

El proceso de enviar datos desde un dispositivo digital, por ejemplo, una computadora, a través de ondas de radio que es un medio analógico, requiere un dispositivo que convierta las señales digitales en ondas analógicas, este dispositivo es el MODEM, el cual se encarga de llevar a cabo este proceso

denominado modulación. En el extremo receptor también es necesario un modem para convertir las ondas analógicas en señales digitales nuevamente, proceso llamado desmodulación.

Para obtener las cuatro velocidades de datos del estándar 802.11b son necesarios tres tipos de modulación:

- Modulación de fase por desplazamiento binario (BPSK) para 1 Mbps
- Modulación de fase por desplazamiento en cuadratura (QPSK) para 2 Mbps
- Modulación de código complementario (CCK) para 5.5 y 11 Mbps

La razón para que sean consideradas velocidades de datos menores a la máxima que ofrece el estándar, se debe a consideraciones de alcance o rango de los dispositivos como veremos mas adelante.

6.1.1 Modulación BPSK para 1 Mbps

Al variar de manera sistemática algunos de los parámetros de la onda analógica, como lo son: amplitud, frecuencia y fase, es posible altrar la codificación, y por tanto la transmisión de la información.

El hecho de que la modulación sea de tipo binaria, nos indica que la entrada a este proceso es un 1 o un 0, por ejemplo los datos no codificados de un

computador. En BPSK solo son posibles dos estados 1 o 0 que se representan en un solo bit de datos. La modulación BPSK es la más básica, y por lo tanto es el tipo de modulación más sólido, debido a esto BPSK es el tipo de modulación para la velocidad de datos base de 1 Mbps. Aunque tiene la desventaja que requiere un numero mayor de transmisiones.

BPSK usa cambios. O desplazamientos, en los tiempos de inicio de una onda para indicar cual de los estados binarios se está codificando. Cada trama de datos que se envía comienza con un preámbulo que establece la línea base para la transmisión y precede a la información real que se transmite. Durante el proceso de reconocimiento en las estaciones emisora y receptora, los dispositivos se sincronizan de manera que se establece una línea de base común. Luego, los cambios en esta línea base o desplazamientos en fase se usan para señalar que cambio de 0 a 1 o de 1 a 0. estos cambios de fase son ventajosos frente a los de amplitud que pueden ser degradados por el ruido de un radio.

Debido a la solidez y confiabilidad de BPSK, es el esquema que se emplea para todos los encabezados de las tramas, sin importar cual modulación se use para la carga de información real.

6.1.2 Modulación QPSK para 2 Mbps

Es una variación de BPSK, donde no se usan simplemente 2 estados 0 o 1. en este tipo de modulación se emplean cuatro representados cada uno por 2 bits: 00, 01, 10 y 11. y se trabaja con la misma línea de base común para la codificación o manipulación. La diferencia es que, el hecho de que se trabaje con el doble de estados que en BPSK, se refleja en el desempeño que también se duplica a 2 Mbps y para esto se requerirá de una señal más clara. El encabezado de trama que se envía mediante BPSK, indica que tipo de modulación manejara la carga, para lo cual se usan técnicas más complejas como QPSK para aumentar el flujo de datos. Cuando ocurre una cantidad excesiva de errores en el envío de la carga usando una técnica de codificación compleja la estación emisora disminuirá progresivamente la velocidad mediante modulaciones más sencillas y más eficaces.

Las velocidades de 1 y 2 Mbps, representan velocidades de desempeño aceptables y normales para dispositivos como lectores de código de barras, y para aplicaciones de transacciones numéricas. Pero en el caso de requerir velocidades más grandes como es el caso de los entornos de oficina se vuelven insuficientes.

6.1.3 Modulación CCK para 11 Mbps

La Modulación de código complementaria CCK, proporciona una velocidad de 5.5 Mbps y una velocidad máxima de 11 Mbps. BPSK trabaja con 2 bits, QPSK

con 4 bits. CCK sigue este patrón exponencial al iniciar con un flujo de datos de 8 bits para alcanzar 11 Mbps, y disminuye hasta un flujo de 4 bits para 5 Mbps.

Por supuesto una transmisión que está modulada dos veces (mas velocidad de datos), requerirá un canal más claro que una que solo lo está una vez (menos velocidad de datos). Lo que se ve reflejado en el rango o alcance de una comunicación. A medida que incrementa la velocidad de datos el rango disminuye. Observe la figura 12.

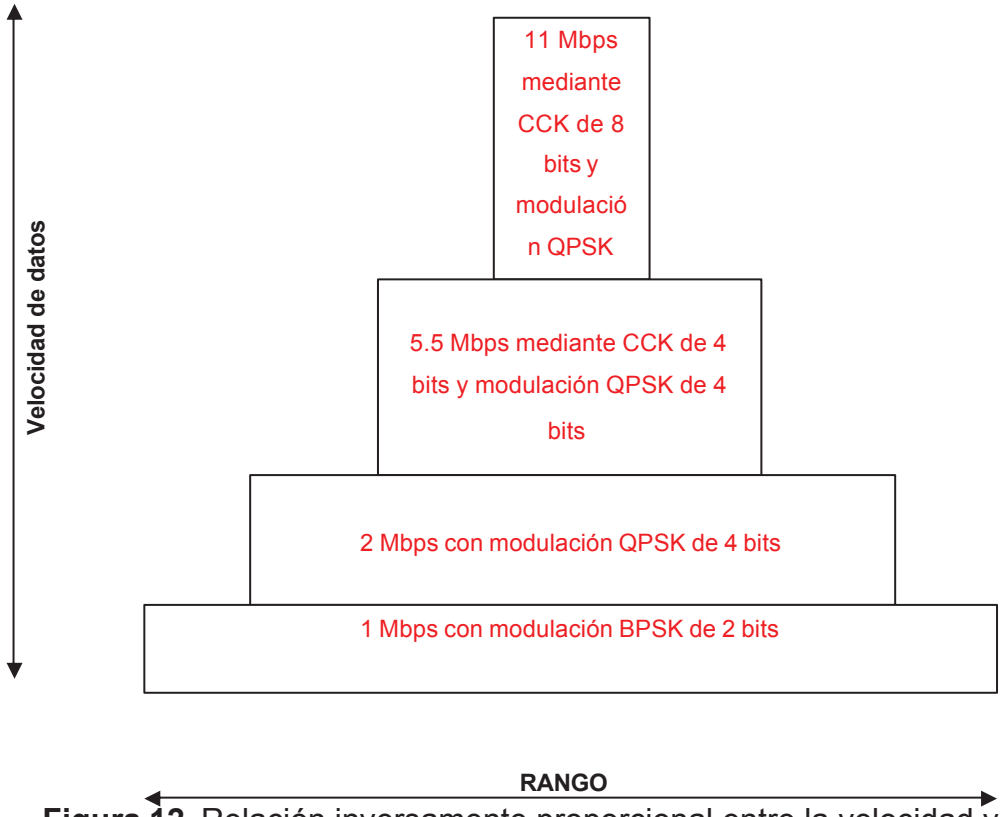

Figura 12. Relación inversamente proporcional entre la velocidad y el rango

6.1.4 Cambio de velocidad

Este termino se refiere a la capacidad que tiene un dispositivo de cambiar en forma dinámica y automática las distintas tasas de velocidades. Esto con el fin de obtener mejores desempeños de acuerdo a las condiciones que se presenten. 802.11b permite cambio de velocidades desde CCK hasta los tipos de modulación QPSK y BPSK.

Este proceso de establecimiento de diferentes velocidades de datos esta basado en el numero de errores que se recibe cuando un paquete se envía a una velocidad de datos determinada con un tipo de modulación especifico. Cuando se rebasa el umbral de errores permitidos, el cliente comienza un proceso de búsqueda de un AP en la misma banda de 2.4 GHz que le proporcione una señal fuerte, si lo encuentra se asocia con él y de ese modo puede mantener la velocidad más alta posible. Pero cuando el cliente es incapaz de encontrar una señal fuerte se iniciará el proceso de cambio de velocidad. Este proceso automático usa de manera progresiva tipos de modulación menos complejos, y por tanto más eficaces, que darán como resultado menos errores, una cobertura geográfica más grande y una velocidad de datos más baja.

6.2 Capacidad de salida

Hasta ahora si creemos que la velocidad de salida lo es todo en un enlace Wi-Fi, pues no es tan importante como la verdadera capacidad de salida a la que se ven limitados los equipos Wi-Fi, debido a que esta si toma en cuenta los errores en la transmisión que son lo suficientemente serios para ocasionar un reenvío y no tan frecuentes como para provocar un cambio de velocidad de datos mas lenta. Por ultimo la velocidad de datos se aplica a todo el medio de transmisión de y no al usuario individual.

Veamos factores que están involucrados y afectan la capacidad de salida:

1. Sobrecarga con respecto a la carga
2. Interferencia
3. Propagación de trayectorias múltiples
4. Método de acceso al medio
5. Umbrales de fragmentación
6. RTS/CTS
7. Encabezado corto
8. Cifrado
9. Selección del fabricante

6.2.1 Sobrecarga con respecto a la carga

En términos generales la sobrecarga se define como los medios para hacer llegar la carga a donde tiene que ir.

En las LAN Wi-Fi, un porcentaje mas alto de paquete de datos completos se utiliza para la sobrecarga del proceso de transacción, dejando una cantidad menor de la velocidad de datos disponible para los datos reales. Así suene raro Ethernet a 10 Mbps es más rápido que Wi-Fi a 11 Mbps. Debido a que el proceso de transmisión de datos a través de RF es inherentemente mas sofisticado que la transmisión por cable. Aquí es donde notamos un degrado de la capacidad de salida por el exceso de sobrecarga.

6.2.2 Interferencia

Como fue señalado anteriormente, los errores excesivos ocasionados por la interferencia, acarrearan el proceso de cambio de velocidad. Sin embargo antes de que se rebase el umbral de errores el dispositivo transmisor seguirá reenviando paquetes. Estos reenvíos tienen el efecto de disminuir la capacidad de salida (la velocidad de datos permanece igual pero el desempeño disminuye).

6.2.3 Propagación de trayectorias múltiples

Las trayectorias múltiples son un fenómeno que evita que el dispositivo receptor obtenga niveles de energía o, en ciertos casos, se utiliza de manera conveniente para mejor la calidad y cantidad de energía que recibe el dispositivo receptor direccionando la energía. Las trayectorias múltiples se ocasionan cuando al propagar una señal desde un dispositivo emisor, esta encuentra varios obstáculos ambientales, comenzando con la atmósfera. Algunos obstáculos actúan como barrera absorbiendo toda la energía de la señal, mientras otros solo reflejan la señal de la misma forma en que un espejo refleja la luz creando imágenes secundarias (trayectorias múltiples de la señal propagada). El material que es mayor causante de trayectorias múltiples es el metal.

En Wi-Fi estas señales duplicadas son señales fantasma, que se reciben en tiempos ligeramente distintos. Este fenómeno ocasiona los datos se tengan que reenviar. Estas retransmisiones toman tiempo, lo que disminuye la capacidad de salida.

Sin embargo los radios Wi-Fi tienen la capacidad de identificar algunas señales reflejadas que son duplicados y las ignoran. Pero esta identificación sólo es posible durante un periodo determinado. Este periodo se conoce como retardo en la propagación. Mientras más grande sea este periodo, será mas largo el periodo en que el radio pueda identificar (ignorar) la señal duplicada, y por tanto mantener el desempeño.

6.2.4 Método de acceso al medio

La mejor forma de acceso al medio, como la es la de utilizar el medio cuando se necesita, después de haber escuchado o sentido el medio antes de comenzar la transmisión. Esto se conoce como el Acceso múltiple con sensor de portadora (CSMA). Esta forma de acceder al medio fue popularizada por las redes Ethernet 802.3 que agrega a CSMA un medio para detectar colisiones o transmisiones incompletas, lo que da como resultado CSMA/CD (detección de colisiones).

Los estándares 802.11 IEEE usan DCF (distributed cordination Function, funcion de control distribuido)), basado en el mismo método de acceso con la diferencia en que no utiliza CD sino CA (Elusión de colisiones), esto debido a las diferencias fundamentales entre el cable y las RF. En el modo DCF para poder transmitir es necesario sentir el medio primero. Cuando el dispositivo transmisor encuentre otro dispositivo que ya ha transmitido, dará un paso atrás y esperara para volver a intentar la transmisión. El tiempo en que un dispositivo vuelve a intentar sentir el medio es aleatorio. La estación emisora continuara este proceso hasta que reciba un paquete de reconocimiento, o ack, desde el destino.

Es así como la elusión de paquetes, los periodos de retroceso aleatorio, y los reconocimientos, dan como resultado el incremento de la sobrecarga y por lo tanto afecta la capacidad de salida.

Aunque CSMA es la mejor forma de acceso al medio, también conlleva serios inconvenientes a la hora de hablar del trafico que requiere baja latencia como lo es la voz y el video. Debido a que CSMA no establece prioridades entre los tipos de trafico. Es posible que mientras se haga una llamada telefónica se escuche entrecortada cuando la estación emisora pierde su acceso al medio mientras otra envía un paquete de correo electrónico.

Para resolver estos inconvenientes, se han desarrollado distintos medios de asignar prioridades, y proporcionar cierto nivel de calidad de servicio (QoS) para nuestra red que serán tratados mas adelante.

6.2.5 Umbrales de fragmentación

El tamaño de la carga para el estándar 802.11 varia de 256 a 2312 bytes. Esto no impide que a través de una red Wi-Fi se transporten cargas mayores a 2.3 KB, como es el caso de videos, música, paginas web. Para este propósito es necesario dividir los paquetes de datos en segmentos más pequeños, o fragmentos. Entre más grande sea el fragmento, la carga estará mejor representada en todo el paquete, incluyendo la sobrecarga. Por esto, mientras

más grande sea el fragmento será mejor el desempeño, debido a que se usara menos espacio para la sobrecarga. El valor típico para el umbral de fragmentación predeterminado es de 2.3 KB que incluye carga y sobrecarga. Para analizar como se afecta la capacidad de salida examinemos la siguiente relación: ‘’La probabilidad de que un paquete sea recibido de manera exitosa es inversamente proporcional a su tamaño’’. Por ejemplo, las frecuencias de radio que no necesitan licencia, mientras más grande sea el paquete habrá más probabilidades de que sea obstruido por la interferencia, ocasionando que no llegue a su destino. Sin embargo la capacidad de salida es mayor cuando el umbral de fragmentación esta maximizado. En entornos ruidosos es necesario fragmentar los paquetes, es decir, se divide un paquete en unos más pequeños, el radio transmisor, los envía en varios paquetes RF y se reensamblan en el radio receptor. Este tamaño más pequeño de los paquetes ocasiona que el tiempo general que se usa para transmitir sea mas corto y existen menos oportunidades de que el paquete se dañe con la interferencia. Cuando se presentan estos entornos ruidosos es necesario un ajuste del umbral de fragmentación para mejorar la capacidad de salida.

6.2.6 RTS/CTS

Esta opción de las redes Wi-Fi ya fue explicada con detalle en el capitulo 4, y en forma resumida se encarga de resolver el problema de los nodos ocultos que es específico en las redes inalámbricas. Despliega un método de control

centralizado que supera el modelo CSMA básico. Sin embargo, al hacerlo introduce un tipo de paquete completamente nuevo para el trafico 802.11 y otra capa de sobrecarga. Es decir cuando RTS/CTS esta habilitado, existe una repercusión en el desempeño. Por esto debe estar habilitado de acuerdo con las necesidades.

6.2.7 Encabezado corto

El encabezado corto es una opción incluida en el estándar 802.11b, la cual disminuye el tamaño de la parte de sincronización de la sobrecarga de la trama, de 128 bits a 56 bits. Es una opción que si esta habilitada (si esta disponible), permite optimizar la capacidad de salida. Debido a que es una opción no estará disponible para todos los fabricantes Wi-Fi y si se ofrece es posible que no este habilitada como valor predeterminado. La única situación es que la opción encabezado corto no debe estar habilitada en entornos mixtos de dispositivos compatibles con 802.11 de 1 y 2 Mbps y es posible que no cuenten con esta opción.

6.2.8 Cifrado

El nivel de seguridad más rudimentario del estándar en estudio se denomina Privacidad equivalente al cableado (WEP). Últimamente esta en desarrollo un

nuevo estándar IEEE para resolver los problemas de seguridad que es el 802.11i.

Tanto WEP como 802.11i proporcionan un método para cifrar paquetes con el fin de proteger el enlace inalámbrico. En WEP las claves utilizadas para el cifrado son estáticas y solo se pueden modificar de forma manual y esta clave es la misma para todos los usuarios de la red. En 802.11i, las claves de cifrado son dinámicas; cambian a una frecuencia que es ajustada por el administrador de red.

Auque los métodos de seguridad mencionados anteriormente ofrecen diferentes niveles de seguridad, el impacto que causan en el desempeño es el mismo: el cifrado y el descifrado de paquetes requiere de poder de procesamiento y ancho de banda, lo que disminuye la capacidad de salida. Por este hecho no es saludable descuidar el aspecto de seguridad por no perjudicar el desempeño.

Si se quiere tener en cuenta la seguridad a la hora de desplegar una red inalámbrica, se debe hacer la selección de un fabricante que también tenga en cuenta la seguridad. El procesamiento del cifrado se puede hacer en el procesador del radio (procesamiento basado en el anfitrión), por ejemplo, el procesador del AP, o de la computadora portátil. El procesamiento de cifrado también se puede hacer instalando un mecanismo de cifrado en la capa MAC

del radio, y con mecanismos de medición de la capacidad de salida se ha encontrado que el desempeño se reduce en un 25 por ciento. Cuando el procesamiento esta basado en el anfitrión el desempeño varía de la capacidad de procesamiento del anfitrión. Cuando se utiliza un mecanismo de cifrado basado en la capa MAC del radio se utiliza un procesador exclusivamente para esta actividad. La reducción del desempeño en este caso solo es del 2 por ciento.

Cada mecanismo de cifrado esta diseñado para procesar un solo algoritmo de cifrado. Hoy día, los mecanismos de cifrado están diseñados para procesar el algoritmo RC4 que esta basado en WEP y en 802.11i.

Existen otras alternativas, como la de configurar un túnel cifrado y seguro a través de una VPN (red privada virtual). Las VPN usan un algoritmo DES (estándar de cifrado de datos) o 3DES (DES triple) y no RC4. El DES requiere de una mayor capacidad de procesamiento lo cual afecta en sobremanera a la capacidad de salida.

Lo anterior nos dice que el desempeño de nuestra red depende del tipo de mecanismo de seguridad que se emplee, entre mas procesamiento requiera, mas se degradará la capacidad de salida.

6.2.9 Selección del fabricante

La capacidad de salida puede variar enormemente de un fabricante a otro. Esta variación puede deberse a la decisión de un fabricante de proporcionar soporte o no para las opciones del estándar, por ejemplo, RTS/CTS o los encabezados cortos, o la inclusión de un mecanismo cifrado en la capa MAC. La selección de otros componentes esenciales, como el modem, o el conjunto de circuitos integrados del radio mismo, tiene que ser cuidadosa para lograr una buena capacidad de salida. Aparte de lo anterior, otros factores de igual o mayor importancia en el propósito de obtener una alta capacidad de salida, son las decisiones de diseño electrónico del fabricante irreconocibles por el usuario final, esto incluye la selección de dispositivos como filtros, amplificadores, osciladores, pueden tener un alto impacto en el desempeño

Por lo anterior es recomendable mirar el producto como una caja negra y observar únicamente la capacidad de salida del sistema y compararla con la de otros fabricantes Wi-Fi.

Como resultado final, varios aspectos pueden afectar la capacidad de salida, desde la selección del fabricante hasta en la forma en que se configuren algunos parámetros. Entonces, ¿cual es la capacidad de salida de un equipo 802.11b?, La respuesta a esta pregunta es que cuando se opera con una velocidad de datos de 11 Mbps y se transfiere trafico de una red de oficina, por

ejemplo, exploración web, correo electrónico y archivos adjuntos, los rangos de la capacidad de salida van desde 4.5 Mbps hasta un máximo de 6.5 Mbps aproximadamente. Es decir debemos esperar el 50 por ciento de la velocidad de datos para cualquiera de estas.

6.3 Alcance en distancia: Rango

El rango de un dispositivo Wi-Fi tiene una dependencia muy fuerte de los factores ambientales, lo que es especialmente importante para las instalaciones Wi-Fi empresariales, factores que pueden variar dependiendo del diseño y materiales de construcción, ocasionando un fuerte impacto en el rango. A continuación se expondrán elementos que contribuyen en el rango de un dispositivo Wi-Fi determinado, como lo son:

Potencia de transmisión

Sensibilidad de recepción

Ganancia de la antena

Diversidad de antenas

Perdidas en el cable

6.3.1 Potencia de transmisión

La potencia de transmisión, puede entenderse como el volumen máximo con el que se puede enviar una onda y su principal variación se da con respecto a la distancia a la que se quiera hacer llegar el mensaje. Mientras más grande sea la potencia de transmisión, será mas fuerte la señal y será más grande la distancia que esta podrá alcanzar (manteniendo las demás condiciones constantes). La potencia de transmisión de los dispositivos Wi-Fi se acostumbra a medir en mW y sus señales recorren decenas de metros.

Un dispositivo Wi-Fi incluirá, además de una capa MAC y un circuito de capa física, un radio principal, que se conoce como RF principal, elementos que conforman el transmisor final que normalmente proporciona una potencia de transmisión de recepción y de salida. A pesar que varia de un fabricante a otro los dispositivos normales Wi-Fi proporcionan una potencia de transmisión de aproximadamente 30 mW. Cuando el dispositivo viene con un amplificador de potencia (PA), este por lo general aumenta la señal en un factor de 3:1, es decir una potencia de 100 mw.

Una unidad muy usada para medir los mW es el decibel (dB), que no solo expresan una medida de potencia, sino también la proporción de potencia o voltaje en términos de ganancia o pérdida.

6.3.2 Sensibilidad de recepción

La sensibilidad de recepción se puede ver de una forma coloquial, como la forma en que el radio Wi-Fi puede escuchar con claridad. Es la medida de la señal más débil que el radio puede recibir y demodular con éxito.

Al igual que la potencia de transmisión la sensibilidad se mide en decibeles. La sensibilidad de recepción normalmente se mide en decibeles negativos debido a que son valores muy pequeños en mW, por ejemplo –10 dB tiene un valor real de 0.1 mW y es el valor de potencia mínimo que el receptor puede escuchar para el ejemplo. La sensibilidad de recepción depende de la codificación que se utilice que determina la velocidad de datos del dispositivo, por lo tanto para técnicas de codificación más estrictas se necesitara una señal más fuerte. Por tanto un radio Wi-Fi de 11 Mbps que proporciona una sensibilidad de recepción de –85 dBm, podría demodular exitosamente una señal mas débil, por ejemplo de –94 dBm, cuando se transmite a solo 1 Mbps con técnicas de codificación mas sencillas.

El piso del ruido (ruido en el ambiente) y la fuerza de la señal también se pueden cuantificar en términos de decibeles negativos. Cuando el valor del piso del ruido excede el valor de la señal recibida, la señal se pierde en el ruido y no se recibe. La diferencia entre el piso del ruido y el valor de la señal se denomina relación señal a ruido (SNR). Por ejemplo, cuando el nivel del ruido en un edificio es de –125 dBm y la fuerza de la señal es de –63 dBm, el SNR

seria de 62 dBm, lo que es un SNR muy bueno. Por otro lado, en un ambiente mas ruidoso con un nivel de ruido de –80 dBm con una señal débil de –90 dBm, el SNR es un numero negativo (-10 dBm), en este caso la señal no se podrá recibir. Entre mas ruidoso sea el ambiente el rango del dispositivo será menor. El valor de SNR para los radios 802.11b, es comúnmente de 10 a 20 dB. De la misma forma que existen los amplificadores de potencia para la potencia de transmisión, también existe la opción de escoger la opción de un amplificador de ruido bajo (Low Noise Amplifier, LNA) para mejorar la sensibilidad de recepción.

6.3.3 Ganancia de la antena

Para un amplificador, ganancia es la proporción de la amplitud de salida de una señal en relación con su amplitud de entrada, la cual normalmente es expresada en decibeles. Para una antena, ganancia es la proporción de su directividad en una dirección determinada comparada con la relación con alguna antena de referencia. Mientras mas grande sea la ganancia, será mas dirección el patrón de la antena.

La ganancia de la antena se agrega al desempeño del rango del sistema de comunicación. Los cambios en la ganancia afectaran a ambos lados del enlace.

Las antenas están diseñadas específicamente para una porción en particular del espectro de frecuencia del radio y las antena de los sistemas Wi-Fi están por supuesto sintonizadas en la frecuencia de 2.4 GHz. Las antenas proporcionan la ganancia al sistema, la cual es en un sentido básico la capacidad de transmitir y recibir energía a través de un conjunto limitado de direcciones. El patrón de cobertura ideal es uno de forma esférica, el cual se presenta en las antenas isotópicas (antena ideal), que son las antenas que se toman de referencia para medir la ganancia de las demás antenas. La ganancia de una antena normalmente se cuantifica en dBis (decibeles comparados con una antena isotópica). Por otra parte, la ganancia de una antena se puede medir en dBd, ganancia relativa a una antena dipolo, la cual a su vez tiene una ganancia de 2.14 dBi. Para convertir un valor dBd a uno dBi, se resta 2.14 al valor dBd. En la tabla 3, se observan diferentes tipos de antenas que se pueden usar en dispositivos Wi-Fi con sus respectivos patrones de cobertura y su ganancia.

Tabla 3. Ganancia típica de antenas para Wi-Fi

Tipo de antena	Patrón de cobertura	Ancho del haz horizontal.	Ganancia aproximada
Omnidireccional	Omnidireccional	360^0	Entre 2 y 12 dBi
Bastidor	Hemisférico	Entre 60 y 80^0	Entre 3 y 9 dBi
Yagi	Direccional	Entre 20 y 40^0	Entre 10 y 15 dBi
Disco parabólico	Haz angosto	Entre 10 y 20^0	Entre 20 y 28 dBi

6.3.3.1 Limitación de la Propagación de RF

Antes de que se implemente cualquier otra medida de seguridad, es importante considerar las implicaciones de la propagación de RF por los APs en una red inalámbrica. Escogidas de una forma inteligente, la combinación adecuada de transmisor/antena puede ser una herramienta efectiva que ayudará a limitar el acceso a la red inalámbrica al área única pretendida de cobertura. Escogidas de forma poco inteligente, pueden extender la red más allá del área pretendida hacia un estacionamiento o más lejos.

Principalmente, las antenas se pueden caracterizar de dos formas-de direccionalidad y de ganancia. Las antenas omni direccionales tienen un área de cobertura de 360 grados, mientras que las antenas direccionales limitan la cobertura a áreas mejor definidas. La ganancia de la antena típicamente es medida en dBi[13] y está definida como el incremento de la potencia que la antena agrega a la señal RF.

Debido a que los productos actuales 802.11 hacen uso de la banda sin licencia ISM (Industrial, Scientific, and Medical) de 2.4 GHz, están sujetas a las reglas promulgadas por la FCC en 1994 para uso de espectro distribuido. Estas reglas especifican que cualquier antena vendida con un producto debe ser probada y aprobada por un laboratorio de la FCC. Para evitar que los usuarios utilicen de

[13] dBi está definida en referencia a una antena teóricamente isotrópica (propagación perfectamente esférica).

forma incorrecta o ilegal antenas con productos 802.11, la FCC también requiere que cualquier AP capaz de utilizar antenas removibles deberá utilizar conectores no estándar.

En los Estados Unidos, la FCC define el máximo de Potencia Efectiva Isotrópica Radiada (Effective Isotropic Radiated Power - EIRP) de una combinación transmisor/antena como 36 dBm, donde EIRP=potencia del transmisor+ganancia de la antena-perdida del cable.

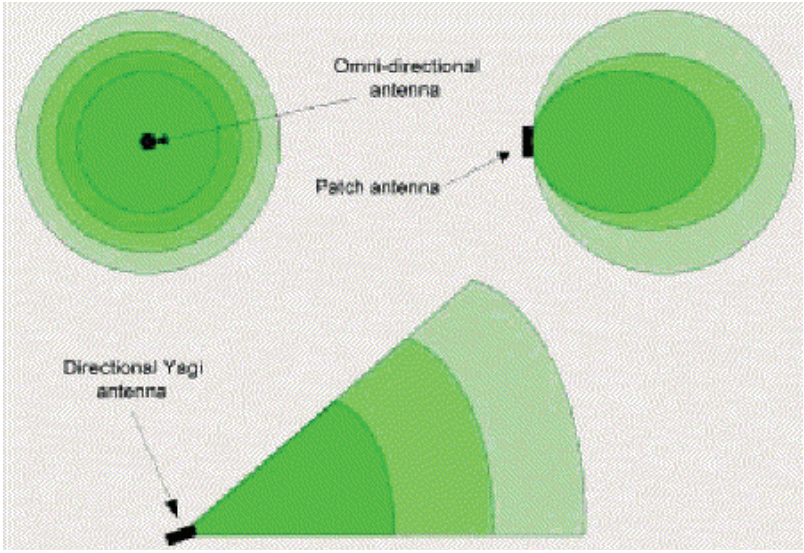

Figura 13. RF patrones de propagación de antenas comunes.

Esencialmente, esto significa que mientras la potencia del transmisor aumenta, la ganancia de la antena debe disminuir para permanecer abajo del máximo legal de 36 dBm. Por ejemplo un transmisor del 100-mW equivale a 20 dBm. Éste transmisor combinado con una antena de 16 dBi produce un total de 36

dBm, que es el límite legal. Para incrementar la ganancia de la antena, estaríamos legalmente obligados a reducir la potencia del transmisor. En la práctica, la mayor parte de las combinaciones transmisor/antena vendidas juntas están por debajo del máximo permitido por la FCC de 36 dBm.

Las implicaciones de todo esto son que las combinaciones del poder del transmisor/ganancia de la antena están estrictamente reguladas y limitan el área que legalmente puede ser cubierta por un solo AP. Cuando esté diseñando una WLAN, es importante llevar a cabo un reconocimiento a fondo del lugar y considerar los patrones de propagación RF de las antenas que se vayan a usar y la potencia efectiva de la combinación transmisor/antena. También como la banda ISM está esencialmente abierta para ser usada por cualquier persona sin licencia, es importante considerar la posibilidad de la negación de servicio (Denial Of Service - DOS) de otras fuentes benignas tales como teléfonos inalámbricos de 2.4 GHz. Finalmente, considerar que un atacante potencial podría no estar jugando dentro de las reglas de la FCC. Un atacante con recursos podría estar usando transmisores de alta potencia, antenas de alta ganancia, y/o receptores más sensitivos. Cada uno de estos puede afectar el rango efectivo de una red inalámbrica.

6.3.4 Diversidad de antenas

Un sistema de diversidad de antenas es el que tiene dos antenas integradas en un solo dispositivo RF, principalmente en el dispositivo receptor. La diversidad

mas usadas en las redes Wi-Fi es la diversidad espacial pasiva. Un sistema de diversidad de antenas esta diseñado para posicionar físicamente la antena en el mejor lugar posible para recibir una señal entrante.

La diversidad de antenas para los dispositivos Wi-Fi están espaciadas de manera optima con 4.5 pulgadas una de la otra que equivale a 11.5 centímetros, alrededor de la misma longitud física de una onda de RF de 2.4 GHz. Tener dos antenas espaciadas una de la otra en un dispositivo estático como un punto de acceso y seleccionar entre las dos de acuerdo a la calidad de la señal recibida es lo mismo que posicionar una sola para recibir una buena señal.

6.3.5 Perdidas en el cable

El cable de antena para los dispositivos Wi-Fi es normalmente el cable coaxial grueso, similar al 10base5 ‘’Thicknet’’ que usa Ethernet o cable de televisión. Las perdidas en el cable se expresan en dB por pie o por metro. A pesar de que las especificaciones de los fabricantes varían, los cables de antena están normalmente divididos en categorías de ‘’perdida baja’’ y de ‘’perdida ultra baja’’, en las cuales el primero ofrece perdidas de aproximadamente 6.7 dB por 100 pies por 330 metros y el segundo cerca de 4.4 dB por 100 pies. En base a lo anterior, se puede notar que si se usa un cable muy largo para la antena se puede perder la mayor parte de la ganancia proporcionada por la antena a la que esta conectado.

Al igual que fue determinada la verdadera capacidad de salida de los dispositivos Wi-Fi llego el momento de definir cual es el alcance en realidad de estos dispositivos teniendo en cuenta las anteriores consideraciones. Además de lo anterior la determinación del rango se hará teniendo en cuenta un entorno de oficinas típico que solo esta relativamente abierto y obstruido por paredes de cubículos parciales en lugar de paredes que van del techo al piso, considerando una velocidad de datos de 11 Mbps y basándonos en una antena dipolo de 2.2 dBi. Con estas condiciones la aproximación del rango esta entre 90 y 150 pies ó 30 y 50 metros, pero lo mas común es de 30 metros.

6.4 Interoperabilidad

Es la capacidad que tienen los dispositivos de diferentes fabricantes para operar entre sí, y esta interoperabilidad es una función de la madurez relativa del estándar y la terminación del estándar en términos de las funciones que pidan los clientes. El estándar 802.11b esta lejos de ser maduro y menos que completo. Además la transmisión a través de ondas RF es un proceso que necesita muchas opciones para el manejo de la información que puede que estén presentes en un fabricante y en otro no lo estén.

Las características descritas anteriormente como los encabezados cortos, RTS/CTS, e incluso el cifrado WEP, son opciones del estándar 802.11b. sin embargo, un fabricante tiene el derecho de decir que es compatible sin

necesidad de contar con ninguna de estas características opcionales. Debido a la naturaleza bidireccional de las comunicaciones de datos, se debe contar con las mismas opciones en ambos lados del enlace para poder aprovechar la característica opcional.

7. SEGURIDAD EN LAS WLANS

7.1 Introducción

Como ya se había mencionado en el capítulo 4, cuando se nombraban algunas características de la capa MAC; la seguridad o securización, llamada así por algunos autores; es una parte a priori en las redes, por lo que vale la pena profundizar en ella.

Los analistas indican que aunque las ventas de dispositivos WLAN están siendo elevadas, no se está produciendo la explosión que se esperaba. Las causas a las que se atribuyen este hecho son fundamentalmente dos; los problemas de seguridad y al desconocimiento de cómo emplear estas tecnologías para aumentar la productividad u otros beneficios inmediatos.

A continuación profundizaremos en las dos partes importantes de la securización, también se hablará del protocolo WEP y algunas recomendaciones relevantes en la seguridad de las Wi-Fi.

7.2 Historia de la seguridad en redes inalámbricas

Existen importantes argumentos por el cual los responsables de las TI iniciaron con una serie de desconfianza con respecto a ésta tecnología. Tras la

publicación de los primeros estándares que determinaron el nacimiento de las redes wireless Ethernet (IEEE 802.11a y b), también denominadas Wi-Fi por el *consorcio*[14] que empuja su implantación y la interoperabilidad de los productos, surgió la necesidad inmediata de proporcionar un protocolo que proporcionase seguridad frente a intrusiones en este tipo de transmisiones y como ya se había dicho, el WEP (Wired Equivalent Privacy) es ésta repuesta. Este protocolo proporciona tres mecanismos de seguridad (por nombre de la red o SSID, por clave estática compartida y por autentificación de dirección MAC) que se pueden utilizar por separado pero que es más recomendable combinarlos. Sin embargo pronto se descubrió que todos ellos eran fácilmente desbloqueados en corto tiempo (incluso minutos) por expertos, utilizando herramientas de escucha en redes (sniffers). Para inhibir un poco este inconveniente, se han diseñado soluciones no estandarizadas apuntando en diferentes áreas. La primera de ellas es sustituir el mecanismo de clave estática por uno de clave dinámica WEP (TKIP u otros), lo que dificulta su identificación, puesto que el tiempo de computación que lleva es mayor que la frecuencia de cambio. Sin embargo debe ser complementada con otras técnicas como sistemas Radius para forzar la identificación del usuario, túneles VPN (red virtual privada) con cifrado IPSEC (Abreviación de Protocolo de seguridad de Internet), o análogo entre el terminal de usuario y un servidor seguro interno para imposibilitar el

[14] La alianza wi-fi es una asociación internacional formada en 1999 para certificar la interoperatibilidad de los productos de redes de área local inalámbricas basados en la especificación IEEE 802.11. la alianza wi-fi tiene unas 200 compañías miembros, alrededor del mundo y cerca de 1000 productos han recibido la certificación WI-FI® desde marzo de 2000. el objetivo de los miembros de la alianza wifi es unir la experiencia con la interoperatibilidad de los productos.

análisis de las tramas enviadas por radio. Los consorcios reguladores, conscientes de la gravedad de esta debilidad y su fuerte impacto negativo en el crecimiento de las WLAN, han propuesto una recomendación provisional denominada WPA (Wi-Fi Protected Access) que conjuga todas las nuevas técnicas anteriormente expuestas.

Desafortunadamente WPA no es el último movimiento ya que realmente es un subconjunto de una especificación final que publicó el consorcio IEEE y que denominó 802.11i (expuesta posteriormente) y que propuso ser la clave definitiva para que las redes LAN inalámbricas sean equivalentes en materia de seguridad a las cableadas como actualmente lo son.

7.3 Problemática en los despliegues de WLANs

Una vez conocidas las inseguridades de las redes wireless, no tardaron en aparecer los ataques. Y una de las más sofisticadas formas se ha denominado "*wardriving*". Consiste en que expertos en redes wireless Ethernet, se desplazan en un coche con un portátil con tarjeta de red inalámbrica y una antena pequeña, realizando una exploración de las frecuencias empleadas por estas redes en zonas empresariales y centros de negocios de grandes ciudades.

La información actual sobre las WLANs, revelan que con mínimo esfuerzo se puede penetrar en una gran mayoría de las redes. Las razones de ello son:

Elevados porcentajes de redes con los parámetros por defecto de los equipos, no activadas las reglas de seguridad básicas o sólo parcialmente, exceso de potencia de señal que permite su fácil recepción desde el exterior, empleados que implantan su propio punto de acceso inalámbrico sin conocimiento de la empresa, seguridad sólo basada en WEP, etc. Solamente una muy pequeña proporción respondía a un patrón de diseño cuidadoso, habiendo introducido mecanismos adicionales de protección (túneles, radius, etc.).

7.4 Autenticación y Cifrado

Cuando se discuten los sistemas de seguridad WLAN, las dos áreas principales son la *Autenticación* y el *Cifrado*, y aunque éstas dos áreas estén muy interrelacionadas, las mencionaremos en ésta sección de manera independiente.

7.4.1. Autenticación

Como mencionamos en el capítulo 4, la autenticación no es más que el proceso en que un dispositivo, es quien dice ser, haciendo uso de un tipo de credencial de identificación.

Los puntos de accesos se pueden configurar de manera que usen contraseñas, las cuales se conocen como *identificadores de Servicio* (SSID, que en

ocasiones también se conocen como ESSID, donde E quiere decir “Extendido”). Algunas personas consideran que los SSID son un medio rudimentario de seguridad, pero en la realidad son muy seguros.

Los puntos de acceso normalmente se distribuyen con un SSID predeterminado que es específico del fabricante (normalmente esta compuesto de una sola palabra) que se emite como parte de las balizas a los puntos de acceso. Cuando ocurre de ésta manera, y un adaptador de cliente tiene configurado un “SSID nulo”, al dejar el SSID en blando (o usar un nombre comodín como “cualquiera” o “ninguno”) en la utilidad de cliente, será capaz de asociarse al punto de acceso.

Las herramientas administrativas como el NetStumbler, incluso el Windows XP de Microsoft, proporcionan la capacidad de registrar todos los SSID que se pueden percibir de un cliente y luego permitir que el cliente se asocie al punto de acceso seleccionado, lo cual es muy agradable para las redes de áreas públicas, como en un sitio donde esté instalada más de una WLAN.

Algunos fabricantes proporcionan la capacidad de eliminar el SSID de las balizas de emisión a los puntos de acceso; por un lado, esto resuelve el problema de seguridad, pero deshabilita la capacidad de que un cliente pueda encontrar la red adecuada con la cual quiere conectarse. Más aún, es común que las personas configuren incorrectamente los puntos de acceso, dejando los SSID en las balizas y emitiendo la contraseña. En pocas palabras, un SSID

debe considerarse más como un nombre de red que una contraseña. Es muy normal que una empresa use el mismo SSID para todos los AP.

Muchos fabricantes Wi-Fi proporcionan la capacidad de restringir el acceso a la LAN basándose en la tabla de direcciones MAC. La programación de direcciones MAC son los únicos identificadores numéricos que usan los fabricantes para los dispositivos LAN como, por ejemplo, las tarjetas de interfaz de red (NIC) que usan cable y las inalámbricas, al igual que los switches, routers, concentradores y puntos de acceso. Los números de direcciones MAC son similares a los números de identificación. Mediante ésta característica, puede introducir un número de direcciones MAC o un rango de direcciones MAC dentro de uno o varios puntos de acceso, por ende sólo permite que los dispositivos que tienen estas direcciones se asocien, o puedan acceder a la LAN. Aun así el enfoque de seguridad en cuanto a las direcciones MAC tiene dos inconvenientes:

Las direcciones MAC pueden falsificarse fácilmente, debido a que algunos adaptadores de clientes usan direcciones de administración universales (UAA), que definen los fabricantes de tal forma que sobrescriba una dirección administrada localmente (LAA). Un pirata informático puede usar un analizador de protocolo inalámbrico para husmear el tráfico inalámbrico y encontrar una dirección MAC válida y luego simplemente copiarla en un adaptador de cliente compatible con LAA, y por lo tanto, hacerse pasar por el cliente legítimo.

Las bases de datos separadas crean problemas administrativos. Cada tabla de direcciones MAC que se ubican en puntos de acceso individuales represente una base de datos separada. Aun cuando algunos fabricantes proporcionan medios para replicar estas tablas a lo largo de un grupo de puntos de acceso, esta solución rompe la sincronización y crea problemas de actualización.

Otra forma en la que se representa la autenticación, es en aquellos dispositivos que contienen certificados válidos para obtener el acceso a la red. Esos certificados no son más que un tipo de autenticación que usan los sistemas de seguridad inalámbricos de algunas empresas de última generación.

Cualquier persona que use una LAN empresarial, ya sea cableada o inalámbrica, está familiarizada con los nombres de usuario y contraseñas para la autenticación.

Otra forma de autenticación para las WLAN es el uso de nombre de usuario y contraseñas también. La autenticación no se lleva a cabo en la capa de aplicación sino en la física misma, lo cual significa que el usuario que no este autenticado no podrá obtener ningún tipo de acceso a la red. Las contraseñas pueden ser permanentes o semipermanentes, es decir, son validas durante un periodo relativamente largo. Otras son las contraseñas para un solo uso (One Time Password, OTP). Estas contraseñas, se generan al escribir un número de identificación personal permanente en una aplicación que entonces genera una

OTP que se aplica normalmente mediante un rango de combinaciones alfanuméricas que pueden ser reconocidas por el servidor de autenticación.

Los distintos medios de autenticación se pueden usar en combinaciones para añadir capas de seguridad. El uso de un numero de identificación personal para obtener un OTP es un ejemplo de esto.

7.4.2 Cifrado

El cifrado es la práctica de cambiar información de forma que se acerque a la imposibilidad de leer el mensaje original, sin la información necesaria para descifrarla. Esta información puede hacer clave, secreto o código. Mientras más complicado sea el código, será mas difícil descifrarlo, y codificar o decodificar la información llevará mas tiempo y capacidad de procesamiento.
Un cifrado o algoritmo es una formula que se usa para generar un flujo de datos cifrados basado en una clave de cifrado. Estas claves de cifrado se pueden medir en términos de longitud y entre mayor longitud tengan el código será más complicado y robusto. La unidad de medida de la longitud de las claves es el bit. Por ejemplo, una clave de cifrado de 40 bits da como resultado 2^{40} combinaciones posibles.

Para crear un mensaje codificado, denominado texto codificado, se combina la clave de cifrado con el mensaje original, o texto simple. Esta operación se hace

mediante una función OR exclusiva (XOR). Existen dos tipos de cifrado. El cifrado de flujo que codifica el texto simple usando 1 bit a la vez, es un cifrado eficiente y rápido. Y el cifrado de bloques que fragmenta el texto simple en bloques y luego los cifra por bloques, agrega un paso mas al proceso, por esto no es tan rápido, pero es más robusto.

Además de la combinación entre la clave de cifrado y el mensaje original, a la codificación se le puede agregar un vector de inicialización, debido a que muchas veces cuando se repite un mensaje por algún error de interferencia, algún pirata puede descifrar la clave por los repetidos intentos, el vector de inicialización sufre cambios constantemente, haciendo que el flujo de información cambie también, evitando que lo descifren.

7.5 WEP (Protocolo equivalente al cableado)

Es el estándar de seguridad inicial de 802.11, el cual entro en desuso por su difícil implementación y sus bajas prestaciones, ya que utiliza claves estáticas que comparten todos los dispositivos de la WLAN. El hecho de que las claves sean compartidas y sea la misma para todos los dispositivos implica que si alguien descifra una sola, podrá fácilmente tener acceso a todo el tráfico de la WLAN. Cuando se da el caso de que sea robado un dispositivo de la red será necesario cambiar el sistema de claves de toda la red y esta es una tarea muy abrumadora, incluso lo es, configurando un medio centralizado que distribuya

las claves de cifrado a todos los dispositivos. Por estas razones la arquitectura WEP, se ajusta solo a aplicaciones pequeñas e inusuales.

WEP utiliza claves de cifrado muy robustas, y están basadas en el algoritmo de cifrado RC4[15] (cifrado 4 de Rivest), el cual es un cifrado de flujo y se puede implementar usando varias longitudes de clave. Es un algoritmo relativamente veloz y de mucha robustez. El algoritmo RC4 es robusto pero los problemas de WEP no pueden atribuirse al algoritmo base.

En WEP, el algoritmo RC4 utiliza claves de cifrado e 40 bits y un vector de inicialización de 24 bits, dando como resultado una clave de 64 bits. Para generar una clave WEP se debe introducir una cadena alfanumérica.

WEP comenzó a quebrantarse, cuando en agosto de 2001, algunos investigadores respetados del campo descubrieron errores en el algoritmo de programación de claves que usa WEP y afirmaron que la claves de 40 bits y aun de 128 bits de WEP que también son posibles pueden ser descubiertas con tan solo la captura de 4 millones de paquetes que se pueden transmitir en cuestión de horas. Y además de esto en poco tiempo apareció una aplicación en Internet llamada AirSnort, con la cual un usuario casual, puede interceptar y descifrar el tráfico WEP. Después de ser publicado el primer ataque con

[15]Cifrado de flujo diseñado por RON Rivest, quien representa a la R en el acrónimo Seguridad RSA, una compañía de seguridad de datos de buena reputación y muy respetada.

AirSnort, comenzaron a aparecer medios más sofisticados de atacar las redes Wi-fi protegidas con WEP.

7.6 El estándar 802.11i

Reconociendo la necesidad de una arquitectura de seguridad mucho más robusta y escalable para las LAN Wi-Fi, el grupo 802.11 de IEEE votó para designar un grupo de trabajo especialmente para la seguridad, la cual ha sido parte de una tarea del grupo dedicado a la calidad de servicio. El grupo de trabajo 802.11i (Tgi en términos de IEEE) se formó en el año 2001, y ha hecho mucho para proporcionar una seguridad empresarial que ofrezca *interoperabilidad*.

Entre otras palabras, el 802.11i especifica a 802.1x, junto con el protocolo de autenticación extensible (EAP), como los medios mediante los cuales los clientes Wi-Fi y las redes se pueden autenticar mutuamente. Lo que es notable acerca del EAP es que el aspecto extensible del protocolo proporciona la flexibilidad de autenticar una variedad de maneras. Esto les ofrece a los fabricantes la libertad de ofrecer diferentes tipos de autenticación o métodos de autenticación usando tipos distintos de credenciales. 802.11i especifica RC4, el mismo algoritmo de cifrado que se usa para las claves WEP estáticas, como el algoritmo de cifrado para las claves dinámicas de cifrado de una sola sesión y un solo usuario.

7.6.1 Tipos de autenticación

Los fabricantes han aprovechado la flexibilidad del esbozo del estándar 802.11i para ofrecer una variedad de tipos de autenticación (también conocidos como métodos de autenticación). Para que una arquitectura 802.11i pueda funcionar, los tipos de autenticación que se usan en el lado del cliente deben ser soportados por el servidor RADIUS debido a que los puntos de acceso están, principalmente, sólo pasando el tráfico de la autenticación de un lado al otro entre el cliente y el servidor, un solo punto de acceso compatible con 802.11i es capaz de funcionar con los dispositivos de cliente que usan varios tipos de distintos de autenticación, suponiendo que estos tipos de autenticación son soportados por el servidor RADIUS. Los servidores RADIUS de algunos fabricantes tienen soporte integrado para múltiples tipos de autenticación, lo cual le permite tener un solo servidor RADIUS que soporte múltiples tipos de autenticación del lado del cliente.

Comenzando el 2001, Cisco System ofreció el primer tipo de autenticación, conocido como LEAP (EAP ligero); con él, las contraseñas son las credenciales de autenticación, habilitando las pantallas de inicio de sesión a la red en el lado del cliente y desplazando a las bases de datos de los dominios de la red. Ya que Cisco es un fabricante de hardware del lado del cliente, originalmente LEAP sólo estaba disponible con los adaptadores de cliente Cisco, pero, ya otros fabricantes tienen la licencia para ofrecerlo.

Como parte del sistema operativo Windows XP, Microsoft añadió un segundo tipo de autenticación alternativo al conjunto 802.11i. El tipo de autenticación protocolo de autenticación extensible con seguridad en la capa de transporte (Extensible Authentication Protocol with Transport Layer Securuty EAP/TLS) se basa en certificados en lugar de contraseñas como credencial de autenticación. Como ya habíamos dicho, la ventaja de un certificado en comparación con una contraseña es que no requiere la intervención del usuario y se pude decir que incluye un grado más alto de seguridad debido a que las credenciales son mucho más aleatorias que las contraseñas seleccionadas por los usuarios. Por otro lado, la autenticación basada en certificados se lleva a cabo en el dispositivo, no a nivel del usuario; entonces un ladrón se puede autenticar en la red si tiene el dispositivo, sin necesitar ningún conocimiento especial. Debido a que EAP/TLS proviene de una compañía de software y reside en el sistema operativo, prácticamente funciona con cualquier adaptador cliente compatible con 802.11i de cualquier fabricante. Esta es una ventaja para los grupos IS que tienen poco, o ningún, control sobre los tipos de hardware de cliente en la LAN lo cual es típico en las inhalaciones universitarias y otras empresas.

Originalmente, EAP/TLS tenía como fin estar disponible sólo en Windows XP, pero Microsoft lo ha considerado, por justicia, y a en el 2002 se dio el proceso para ofrecer EAP/TLS para otros sistemas operativos (incluyendo a W 98, W 2000 y varias formas de Windows CE) como parte de paquetes de servicio que se pueden descargar.

Otros fabricantes han ofrecido tipos de autenticación alternativas, incluyendo el método de autenticación EAP con Capa segura de transporte túnel (Extensible Authentication Protocol with Tunneling Transport Layer Security, EAP/TTLS) que está integrada a la utilidad de seguridad de cliente Odyssey de Funk Software. Meetinghouse Software ha ofrecido un tipo de autenticación EAP/TTLS similar, integrado en la utilidad de cliente Aegis. En EAP/TTLS, se configura un túnel seguro de autenticación en la Capa 2 entre el cliente y el punto de acceso usuario TLS. Una vez establecido el túnel seguro, entonces EAP/TTLS funciona a través de él, permitiendo que se envíen y reciban una variedad de credenciales de autenticación, incluyendo contraseñas y certificados, a través del túnel seguro. EAP/TTLS es un subconjunto de EAP/TLS debido a que sólo usa TLS en el lado del servidor pero no en el del cliente. Sin embargo al proporcionar la autenticación de contraseñas a demás de certificados, EAP/TTLS es una especia de EAP/TLS mejorado.

Una alternativa más reciente a EAP/TTLS es el Protocolo de autenticación protegida extensible (Protected Extensible Authentication Protocol, PEAP), el cual es similar a EAP/TTLS en el sentido de que también establece un túnel para la autenticación, permitiendo el uso de una variedad de credenciales e autenticación. Una implementación inicial de PEAP en los productos Cisco proporciona soporte para OTP con el fin de ofrecer una versión aún más robusta de la autenticación a nivel de usuario.

Para soportar estos tipos de autenticación en el lado del cliente, se requiere, desde luego, el soporte del servidor RADIUS. El servidor de control de acceso de Cisco proporciona soporte para los tipos de autenticación LEAP y EAP/TLS. El servidor Windows XP de Microsoft soporta EAP/TTLS, mientras que el servidor RADIUS Merit de Interlink proporciona soporte para LEAP. Muchos servidores RADIUS proporcionan capacidades de recuperación de fallas, lo cual significa que si se recibe un tipo no soportado de autenticación, pasará la autenticación a otro servidor RADIUS, cuando está disponible. De esta forma puede tener un solo servidor RADIUS o incluso múltiples servidores RADIUS para proporcionar soporte de respaldo a todos los tipos de autenticación del lado del cliente. Como lo muestra la figura, esto le ofrece una variedad de opciones para desplegar una arquitectura de seguridad que proporciona interoperabilidad.

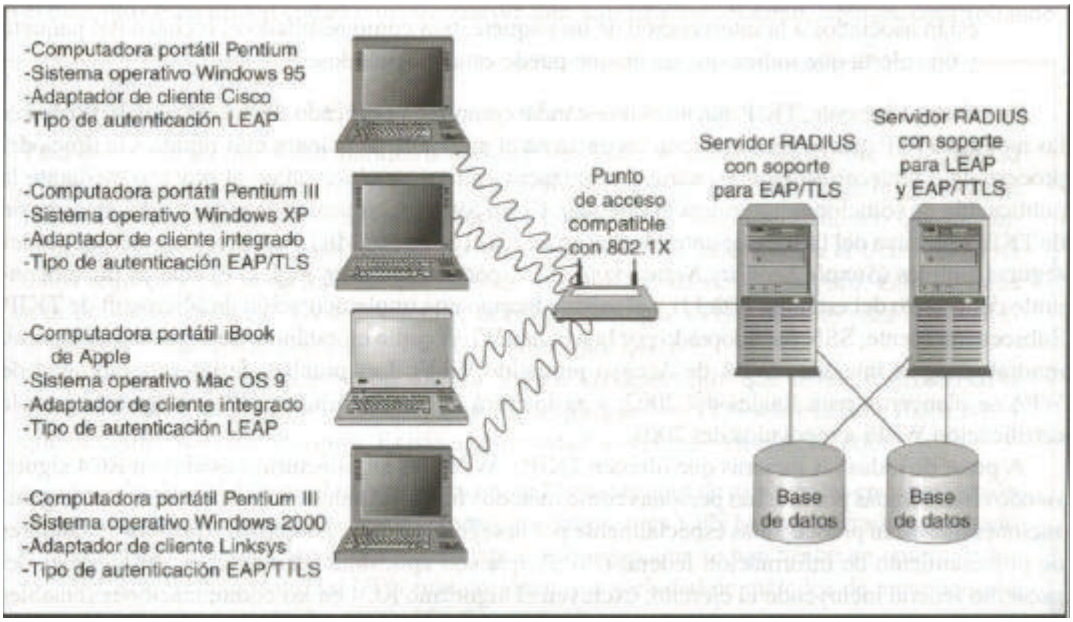

Figura 14. Esbozo del estándar 802.11i, con soporte simultaneo de sistemas operativos, adaptadores de cliente y tipos de autenticación en el lado del cliente

7.6.2 Solución al problema de cifrado WEP

Los distintos tipos de autenticación que se describieron anteriormente representan una gran parte de la necesidad de proporcionar los métodos de autenticación que proporcionen la interoperabilidad que se requiere para escalar la seguridad a niveles empresariales. Sin embargo, no resuelven todas las limitaciones de la implementación 802.11 del algoritmo RC4- Esta deficiencia en la seguridad basada en los estándares para la LAN Wi-Fi no se ha ignorado.

El Protocolo de integridad de clave temporal *(Temporal Key Inlegrity Prolocol. TKIP*) es un medio parcial para "disminuir" las deficiencias de la implementación de RC4 en 802.11 para las claves de cifrado estáticas y, aun más importante, dinámicas. A finales del 2002, TKIP permaneció como un elemento definido de manera general en el esbozo del estándar 802.11i. TKIP también se basa en RC4 y está formado esencialmente de tres mejoras importantes en relación a la implementación inicial del algoritmo:
Combinación de clave por paquete. La clave de cifrado se combina con la dirección MAC de la estación emisora y un numero de paquete secuencial para complicar aún más la clave básica, haciéndola más difícil de romper.

Un vector de inicialización de 48 bits. El doble de la longitud del vector de inicialización de 24 bits original que se especificó en el estándar WEP inicial.

Se recuerde que las longitudes de la clave tienen un efecto exponencial; mientras que una clave de 24 bits tiene aproximadamente 16 millones de combinaciones, una clave de 48 bits proporciona cerca de 280 billones de combinaciones. La longitud más larga de esta clave, junto con la combinación de clave por paquete, hace que las claves de cifrado sean varios órdenes de magnitud más robustas que las implementaciones de generaciones anteriores.

Comprobación de integridad de mensaje *(Message Integrity Checks, MIC).* Está diseñada para frustrar los ataques inductivos o de hombre en el medio. La implementación MIC en TKIP es una versión de la siguiente generación llamada (de forma suspicaz) "Michael". Mediante un MIC. las direcciones de envío y recepción además de otra información única, se integra en la carga cifrada. Los cambios en esta información, que están asociados a la intercepción de un paquete, dan como resultado el rechazo del paquete y una alerta que indica que un ataque puede estar fraguándose.

Se buscaba ofrecer las mejoras TKIP que se necesitan con urgencia en el mercado, de manera más rápida a la típica del proceso de establecer estándares, varias organizaciones han creado un atajo al proceso mediante la publicación de soluciones anteriores al estándar. Cisco Systems ha puesto en el mercado una versión de TKIP exclusiva del fabricante antes de que aparezca el estándar.

Microsoft ofrece el método Redes seguras simples *(Simple Security Networking, SSN*), el cual es un subconjunto del esbozo del estándar 802.11i y al mismo tiempo una implementación de Microsoft de TKIP. Subsecuentemente, SSN fue adoptado por la Alianza Wi-Fi como un estándar de seguridad temporal, renombrando la iniciativa WPA de Acceso protegido Wi-Fi. Las pruebas de interoperabilidad de WPA se planearon para finales del 2002, y se incluyó la compatibilidad WPA obligatoria para la certificación Wi-Fi a mediados del 2003.

A pesar de todas las mejoras que ofrecen TKIP y WPA, las arquitecturas basadas en RC4 siguen siendo consideradas por muchas personas como métodos fundamentalmente insuficientes para organizaciones que están preocupadas especialmente por la seguridad. Por ejemplo, los distintos Estándares de procesamiento de información federal (FIPS), que son aplicables para muchas aplicaciones del gobierno federal incluyendo el ejército, excluyen el algoritmo RC4 en las comunicaciones sensibles que no son secretas. Por extensión, los aspectos de seguridad del Acto de contabilidad y portabilidad de seguridad en la salud de 1996 (HIPAA), determina que la información del paciente debe estar sujeta a la seguridad que ofrece la tecnología de punta; una definición que difícilmente se puede aplicar al algoritmo RC4 y mucho menos a WEP.

Por otro lado, el estándar FIPS-197, publicado en noviembre del 2001, define el Estándar de cifrado avanzado (AES), un estándar de cifrado de la siguiente generación que se basa en las claves de 128 bits de longitud (como mínimo) generadas por el algoritmo Rijndael. Se cree que la compatibilidad con HIPAA siga a FIPS y por tanto es posible que AES reciba la compatibilidad HIPAA. Este desarrollo se mantiene en tendencias de la industria más amplias: los fabricantes de redes privadas virtuales (VPN) quienes durante un largo tiempo han usado el mandato federal del Estándar de cifrado de datos *(Data Encryplion Standard. DES,* y el posterior 3DES o "DEStriple") están migrando a AES como un estándar de cifrado de la generación siguiente.

Existe un acuerdo general entre estos fabricantes que se enfocan a las ofertas Wi-Fi empresariales de que AES es e! estándar de cifrado de la siguiente generación para la transmisión WLAN.

Dado que RC4 es menos robusto que DES o 3DES, y que DES y 3DES son menos robustos que AES, significa que mediante la adopción AES, la industria Wi-Fi prácticamente logró alcanzar una nueva generación de seguridad.

Es posible que la migración a AES no sea tan sencilla como parece a primera vista, y es posible que en realidad no sea una migración completa. Como señalamos ya, que el cifrado tiene un impacto significativo en el desempeño de la red, en especial cuando se implementa en el software y se procesa en el

anfitrión. Cuando el algoritmo RC4 relativamente "ligero" se implementa en el software, el impacto en el desempeño puede exceder 25 por ciento. Un algoritmo Rijndael implementado de la misma forma produce un impacto en el desempeño de 50 por ciento. Por tanto, el escenario más probable es que el algoritmo RC4 (con las mejoras TKIP y WPA asociadas) coexistirá con el estándar AES. Los fabricantes están planeando mejoras a las balizas 802.11 que ofrecerán las capacidades de seguridad del dispositivo lo que permite que los dispositivos asociados negocien el nivel más alto de seguridad que es mutuamente posible. Los fabricantes están, además, desarrollando implementaciones AES basadas en el hardware que posiblemente estarán disponibles a mediados de este año. De forma muy parecida en que los mecanismos de cifrado basados en hardware proporcionan un desempeño mejor para el WEP basado en RC4, estos métodos de cifrado proporcionan la ayuda aún más necesaria de AES basado en Rijndael, brindando así un nivel más alto de seguridad con un impacto mínimo en el desempeño.

Para concluir con esto de la seguridad, podemos agregarle un punto de esperanza y hasta de satisfacción y agradecimiento, por lo que los empresarios de las WLANs han hecho. Si es cierto que e un trabajo dispendioso y fuerte, pero los resultados ya se ven reflejados en las posibilidades o no! Mejor dicho, en lo que dentro de muy poco será nuestro entorno... ¡una sociedad inalámbrica!.

Se recomiendo antes de realizarse un despliegue, que se consulte mayor información para crear una arquitectura de seguridad más exitosa, escalable y robusta; debido a la turgente evolución que éstas llevan.

8. CALIDAD DE SERVICIO (QOS) EN LAS LAN INALÁMBRICAS

Como hemos mencionado en capítulos anteriores, en las WLAN's 802.11 el método de acceso al medio utilizado es DCF (Función de control distribuido) basado en CSMA/CA, en el cual todos las estaciones interconectadas tienen la misma probabilidad de acceder al medio, lo cual significa que ninguna estación tiene una prioridad de importancia mayor que otra.

Lo anterior quiere decir que si todas las estaciones tienen igual prioridad, entonces la información también tiene una prioridad igual. Por ejemplo en una universidad, un mensaje urgente de los directivos a los profesores tiene la misma prioridad que un archivo de audio que esta descargando un alumno desde Internet. Por esta razón, existen algunos tipos de paquetes que deben tener una prioridad mas alta que otros. La capacidad de proporcionar estos distintos niveles de prioridad, y por lo tanto distintos niveles de desempeño, se conoce como calidad de servicio (QoS).

Teniendo en cuenta solo los estandares IEEE 802.11 actuales, Qos no es soportado para las aplicaciones de voz y video, aunque es posible en las redes que tienen cargas muy ligeras.

8.1 Tráfico sensible al tiempo

Se deben establecer paquetes de mayor o menor prioridad que otros. Esto se conoce como clase de servicio (Class of Service, CoS). El tráfico se jerarquiza en niveles.

El tipo de tráfico que requiere del menor nivel de prioridad se conoce como asíncrono, es decir, no tiene requerimientos temporales. El trafico de este tipo son, por ejemplo, correo electrónico, transferencia de archivos y exploración de paginas Web, este trafico puede llegar en cualquier momento que haya disponibilidad en la red.

El tipo de tráfico que tiene un mayor nivel de prioridad, como el tráfico de video y audio, se conoce como isócrono, es decir, que debe llegar a la estación receptora con una velocidad parecida o igual a la velocidad con la cual fue enviado y en la secuencia adecuada.

El tipo de tráfico que requiere mayor nivel de prioridad se conoce como sincrónico, es un tipo de trafico en los que el inicio de u proceso depende de la terminación de otro, por ejemplo, la voz interactiva.

Los estándares IEEE que cumplen con CoS son , entre otros, el 802.1Q y el 802.1D. El 802.1Q define una forma para establecer colas de ‘’prioridad’’

separadas para diferentes tipos de tráfico. El 802.1D proporciona un medio para entregar en forma expedita el tráfico QoS a través de los enlaces de puente, dando solución al problema de enviar rápidamente el tráfico sensible al tiempo a través de un enlace inalámbrico.

Los estándares 802.1Q y 802.1d utilizan etiquetas CoS conocidas como etiquetas 802.1p y están especificadas en los encabezados de paquetes definidos los estándares 802.1Q y 802.1D. Estas etiquetas tienen ocho niveles de prioridad, descritos en la tabla 4, que se asignan en tres bits, para hacerlas relativamente pequeña y eficientes con respecto a la red.

Además de las etiquetas, los paquetes IP pueden llevar también un punto de código de servicio diferenciado (Differented Service Code Point, DSCP), y un elemento de la iniciativa de servicios diferenciados (diffserv) que es parte de IPv4. DSCP es de 6 bits por lo tanto proporciona 64 niveles de prioridad (mas de lo que se necesita).

Tabla 4. Definición de las etiquetas 802.1Q y 802.1D

Etiqueta de prioridad CoS	Tipo de Paquete 802.1Q	Tipo de Paquete 802.1D
7	Reservado para la red	Voz
6	Reservado para la red	Voz

5	Voz	Video
4	Conferencia de video	Video
3	Señalamiento de llamadas	Sonda de video
2	Datos de prioridad alta	Mejor esfuerzo
1	Datos de prioridad media	Mejor esfuerzo
0	Datos de prioridad baja	Mejor esfuerzo

8.2 Prioridad del Tráfico

Ya establecida la forma en que Wi-Fi identifica la prioridad de los paquetes, entonces los dispositivos enviaran los paquetes basados en la importancia del tiempo en que estos deben llegar.

Existen varias formas para determinar si una estación o paquete tiene prioridad, las cuales por su naturaleza pueden ser: estadísticas o determinísticas. Cuando la prioridad es estadística, existe la posibilidad y no es muy seguro que un paquete sensible al tiempo sea tratado con alta prioridad. Cuando es determinística, el punto de acceso se encarga del rol controlador, y programa el orden de transmisión de los paquetes. La asignación estadística conlleva menos sobrecarga que la determinística

8.2.1 Estándares que proporcionan QoS: 802.11e IEEE y WME

El estándar IEEE 802.1e como ya hemos visto antes en un de los primeros de la familia IEEE, debido a su atrasada ratificación, surgió WME (Wireless

Multimedia Extensions, Extensiones multimedia inalámbricas), el cual es básicamente es un subconjunto de 802.11e.

WME busca impulsar un estándar que se pueda implementar de la manera mas cercana a 802.11e para ofrecer QoS a los clientes, antes de que se ratifique el 802.11e. WME es similar al estándar de seguridad SSN/WPA del capitulo anterior.

Dependiendo de que tan necesario sea WME, cuando sea ratificado el 802.11e

8.2.2 Función mejorada de control distribuido

La función mejorada de control distribuido (Enhaced Distributed Control Function, EDCF). Como hemos visto DCF va de la mano de CSMA/CA, y proporciona un uso muy eficiente del ancho de banda disponible, pero no proporciona ningún medio para priorizar el tráfico. EDCF resuelve esta limitación proporcionando nuevos parámetros a los medios inalámbricos. En DCF solo existe una categoría de acceso al medio. EDCF define cuatro categorías de acceso adicionales, como se muestra en la tabla 5, las cuales se asignan a las ocho prioridades QoS definidas en 802.1D (que a su vez se pueden asignar a las de la especificación 802.1Q). Las funciones DSCP, de los encabezados de los paquetes IP, pueden asignarse con etiquetas 802.1D, las cuales, a su vez, pueden asignarse a una categoría de acceso. Estas cuatro

categorías de acceso representan cuatro colas unidifusión adicionales sobre, y por encima, de la cola unidifusión DCF (que tiene prioridad mas baja)

Tabla 5. Asignación de las categorías EDCF a las CoS de 802.1D

Prioridad CoS 802.1D	Prioridad EDCF	Designación EDCF
7	3	Voz
6	3	Voz
5	2	Video
4	2	Video
3	1	Sonda de video
2	0	Mejor esfuerzo
1	0	Mejor esfuerzo
0	0	Mejor esfuerzo

Para hacer posible la asignación de prioridades dentro de categorías de acceso EDCF, se deben ajustar varios parámetros. Como se explico antes, CSMA/CA evita las colisiones basado en que las estaciones tengan tiempos de retraso aleatorio entre sus transmisiones. Con DCF, todas las transmisiones, tienen las mismas prioridades y seleccionan un tiempo de retardo dentro del mismo rango. Con el uso de EDCF, las colas de transmisión de prioridad mas alta pueden seleccionar los tiempos de retardo de un rango de menor duración que los tiempos de retardo de las colas de prioridad más baja. De esta manera las colas de prioridad mas alta, tienen mayor acceso al medio y entregan sus paquetes con una velocidad mas estable y rápida que las estaciones con prioridad baja. Este rango de tiempos de retraso se conoce como ventana de contención, periodo durante el cual una estación pelea con otras para tener acceso al medio. A cada cola de prioridad se le asigna un valor de ventana de contención mínimo, llamado CWmín, y uno máximo, llamado CWmáx. Mientras

mas bajos sean los valores CWmín y CWmáx, serán mas cortos los tiempos de retraso disponibles en el rango y se dará más prioridad a los paquetes de la cola.

Otro parámetro que se puede ajustar mediante distintas categorías de acceso para proporcionar diferentes grados de prioridad es el Espacio arbitrario entre tramas (Arbitrary Inter Frame Space, AIFIS). El AIFIS es la cantidad de tiempo que una estación permanecerá en estado de espera entre la transmisión de tramas o paquetes. Mientras más corto sea el AIFIS, la estación podrá transmitir mas continuamente y sin interrupciones. El AIFIS se debe manejar con la precaución de no establecerlo tan corto por que puede bloquear la transmisión de las demás estaciones incluso la de una con mayor prioridad, hasta que no termine su transmisión.

Todos los parámetros descritos anteriormente como el CWmín, el CWmáx y el AIFIS pueden ser revelados por un AP que use EDCF. Además de estos, existen otros como los limites de Oportunidad de Transmisión (Transmit Opportunity, TxOP), la cuota TxOP y la información de carga. Estos seis parámetros son específicos para cada categoría de acceso de EDCF, como son cuatro, entonces cada AP compatible con 802.11e o WME revelará un total de 24 parámetros. La oportunidad de transmisión es la cantidad de tiempo que un punto de acceso proporciona a la estación emisora cada vez que esta obtiene el control del medio para enviar un paquete. Los limites de TxOP son la

cuantificación de este periodo. Las cuotas TxOP son la cantidad del número de límites TxOP que tiene disponible el AP por cada categoría de acceso. La información de carga del AP, contiene la cantidad de estaciones asociadas con cada categoría de acceso y el uso que estas le pueden dar a los recursos disponibles por parte del AP.

TxOP y la información de carga son útiles para propósitos de control de admisiones. El control de admisiones permite al cliente o AP elija el inicio de una acción basándose en la disponibilidad de los recursos dentro de una categoría de acceso.

El control de admisiones permite que los dispositivos de la WLAN puedan solicitar una cierta cantidad de recursos disponibles para realizar una acción en particular antes de iniciarla, si no se puede, no se hace, y esto proporciona un nivel de calidad mas alto.

8.2.3 Función híbrida de control (HCF)

El DCF usado con CSMA/CA como método de acceso al medio, lo hemos venido mencionando en este y en el capitulo 6, y como sabemos es un protocolo obligatorio dentro de las especificaciones de 802.11. En el estándar 802.11 IEEE, existió también otro protocolo del mismo tipo, pero que se usaba en diferentes condiciones y no era de carácter obligatorio, este es el PCF

(Función de Punto de Control), el cual es aplicable para el tráfico de latencia baja, por ejemplo, el de voz y video. El método ofreció un nivel determinístico de QoS en las LAN Wi-Fi. Las implicaciones en el desempeño y dificultades asociadas a la implementación PCF contribuyeron a su desaparición. La Función de control híbrida (Hybrid Control Function, HCF), se encarga de resolver los requerimientos que implicaron la arquitectura PCF. HCF introduce un nivel determinístico QoS en las WLAN para controlar los requerimientos del trafico más sensible al tiempo como, por ejemplo, las conversaciones de voz sincrónicas. En comparación con EDCF que proporciona un nivel estadístico para el acceso al medio, HCF maneja una QoS mas absoluta, lo que en general proporciona un nivel mas alto de calidad.

Para su propósito HCF incorpora un conjunto de paquetes de administración denominado tramas de acción, las cuales contienen especificaciones de transmisión (Tspec). Las Tspec toman la forma de solicitudes Tspec del cliente y respuestas Tspec del AP.

Para poder proporcionar QoS en Wi-Fi, se requiere de la existencia de la funcionalidad RTS/CTS (descrita en el capitulo 6), debido a que los problemas de los nodos ocultos son mas agudos cuando se presenta el trafico sensible a la latencia.

Una solicitud Tspec contiene información sobre los requerimientos de calidad de un flujo de transmisión en espera. Por ejemplo para una llamada telefónica,

una solicitud Tspec se enviaría desde un cliente a un AP durante el establecimiento de la llamada. El Tspec alojaría la información sobre la cantidad del tiempo que debe transcurrir entre la transmisión de paquetes de voz y la velocidad de datos con la que el cliente enviará estos paquetes. Luego, el AP enviaría una respuesta Tspec al cliente con: una captación incondicional a la solicitud del cliente, un rechazo total (por ejemplo, un tono de ocupado), o una aceptación incondicional con modificaciones en la solicitud. Una vez que el Tspec de respuesta del AP ha sido acptado por el cliente, el AP comienza a enviar al cliente TxOP regulares con intervalos, y de una duración especifica en el Tspec.

9. 802.11 Y ULTIMA MILLA

9.1 802.11 como ultima milla para la derivación lateral de la fibra

Una de las arquitecturas que han ofrecido algunos de los principales proveedores de equipo es la conexión de nodos de *fibra* a MxU. A pesar de que las redes troncales de fibra están casi omnipresentes en todas las áreas metropolitanas principales, vincular una conexión de fibra entre una red troncal y un sitio MxU. incluso en distancias cortas, no requiere menos de 90 días y puede tomar hasta 6 meses con un costo que puede exceder 1 millón de dólares por milla.

La conexión de puentes 802.11 a un nodo de fibra, el cual a su vez se comunica con un dispositivo de punto a punto en un sitio MxU o a un arreglo pequeño de puentes de punto a multipunto 802.11, es una arquitectura atractiva. Resuelve una variedad de aspectos de manera muy elegante:

El proveedor de fibra no puede acceder a los edificios grandes lo suficientemente rápido

El proveedor de servicios BBFW a menudo requiere de un despliegue de tubería muy largo

Los inquilinos de los edificios grandes desean no tener que tratar con la compañía telefónica local

9.1.1 El proveedor de fibra no puede acceder a los edificios grandes lo suficientemente rápido.

Uno de los problemas más grandes para los proveedores *de* fibra es el aumento de la extensión de la penetración de su mercado. La fibra casi siempre se despliega en áreas en donde existe competencia por parte de los servicios DSL y tiene ventajas importantes tanto en costo como en velocidad en comparación a DSL. La conexión es costosa y consume tiempo, además es razonablemente sencillo conectar un edificio mediante un puente 802.11 hacia un nodo de fibra usando un dispositivo como el chasis 15456 de Cisco. De hecho, Cisco ofrece un puente 802.11 como una opción integrada de su direccionador 15454. Esta arquitectura proporciona el acceso inmediato a edificios grandes dentro de un radio de 2 a 5 millas, asumiendo que no existen problemas en la transmisión rectilínea directa. Para las arquitecturas de punto a punto, asumiendo que el proveedor de servicios tiene una elevación adecuada, los edificios se pueden acceder con distancias de 20 millas o más en conexiones de punto a punto con velocidades de 11 Mbps usando radios 802-11, y también a velocidades más altas con los radios 802.11g y 802.11a.

9.1.2 El proveedor de servicio BBFW a menudo requiere de un despliegue de tubería muy largo.

Uno de los retos más importantes para los proveedores de servicios es añadir correcciones a las arquitecturas de punió a punto o punto a multipunto. Tener el acceso a los nodos de fibra prácticamente elimina este problema y además descarta la necesidad de contratar una línea de cobre de la compañía telefónica local, lo cual tiene un efecto material en la rentabilidad de los proveedores de servicios (es decir, la contratación de fibra es generalmente menos costosa que la de cobre).

9.1.3 Los inquilinos de los edificios grandes desean no tener que tratar con la compañía telefónica local

LOS inquilinos MxU que usan los servicios de las compañías telefónicas para obtener una banda ancha DSL, generalmente pagan un costo alto para velocidades que normalmente son menores a las que ofrece una arquitectura 802.11/fibra híbrida. Los ahorros en costo son importantes y la transferencia al acceso 802.11/fibra se puede llevar a cabo en un periodo muy corto, a menudo en menos de una semana.

9.2 802.11 para la extensión de DSL y cable

Un uso interesante de los puentes 802.11 es, y continuará siendo, la extensión de las áreas de servicio que ofrecen los operadores DSL y de módem de cable. Un enlace de punto a punto se puede instalar al extremo de un área de servicio

DSL o de cable y extenderlo a otras áreas que pueden estar tan lejos como 20 o más millas de distancia. Esto elimina la necesidad de conectar o contratar líneas de cobre de otro proveedor, lo cual requeriría de una cuota mensual continua.

A menudo, los enlaces 802.11 de punto a punto se pueden amortizar a lo largo de aproximadamente 90 días. Esta es una mejora importante en los ciclos de amortización de 18 a 24 meses que son comunes a los enlaces MMDS y otros enlaces licenciados. Obviamente, una vez que el equipo ha sido pagado, los gastos de operación mensual del equipo se reducirán significativamente.

Los operadores DSL y de módem de cable también pueden usar un enlace 802.11 de punto a punto como un medio temporal hasta que puedan desplegar su infraestructura de cobre y otro equipo necesario. Dado que el equipo 802.11 no está restringido a ninguna ubicación física como sería el caso de un enlace licenciado (aunque algunos enlaces licenciados se pueden volver a desplegar en nuevas áreas geográficas), es posible instalarlos en otros sitios una vez que la banda ancha de fibra o de cobre estén disponibles. De acuerdo a lo anterior, el hecho es que a los administradores de red normalmente no les agrada desmontar los enlaces incluso si existe una opción de un enlace más rápido disponible ya que el enlace 802.11 se puede quedar en su lugar para propósitos específicos del negocio, tráfico o redundancia.

9.3 Consideraciones prácticas para usar 802.11b como la última milla

La cantidad de cuentas 802.11b que se han vendido en el mercado no es considerable y puede representar tanto como un 30 por ciento de todas las ventas de 802.11b. Es común que los fabricantes con reputación alienten a los clientes prospecto a abandonar, o al menos revisar, sus expectativas con respecto al uso del estándar 802.11 para el uso de la última milla.

Comenzaremos por describir los conceptos básicos que se aplican a las arquitecturas de punto a punto (con frecuencia conocidas como pt-pt) y punto a multipunto (llamadas pt-mpt). Un puente pt-pt es el más simple: sólo se relaciona con dos puntos de extremo. Mientras que una arquitectura pt-mpt involucra un puente principal (denominado *puente raíz)* y aproximadamente cinco puentes que no son raíz, A pesar de que el estándar soportará muchos más puentes en una arquitectura pt-mpt, la conexión para el derecho de transmitir estará imposibilitada para dar servicio, debido a que los puentes están conectando LAN distintas, las cuales a su vez incluyen a cientos, sino es que miles, de usuarios adicionales.

A pesar de que un puente raíz normalmente usará una antena omnidireccional, los puentes que no son raíz casi siempre usarán antenas parabólicas. Los enlaces de puentes de punto a punto casi siempre emplean antenas parabólicas con el fin de maximizar la ganancia, lo cual implica un margen de enlace a enlace directo, velocidad de transmisión/recepción, tasa de errores de

bits y confiabilidad. Las ventajas de usar un haz angosto en lugar de irradiar la energía en direcciones en las que no existen receptores no son poco considerables.

9.3.1 Amplificadores

Una de las preguntas comunes que se hace a los fabricantes de equipo 802.11 es ¿puedo usar un amplificador en mis puentes?. La regulación 15.204 de la FCC establece "Los amplificadores externos de potencia de la frecuencia de radio no deben venderse como productos separados...". La también dice "Sólo la antena con la cual un radiador intencional (transmisor) que está autorizada originalmente se puede usar con el radiador intencional". Lo que esto significa es que cuando un amplificador se debe conectar al radio entre el transmisor y la antena, debe ser proporcionado por el fabricante del equipo; el fabricante a su vez debe tener certificada esta configuración por la FCC, y el amplificador debe venderse con el otro equipo y no como un dispositivo opcional.

9.3.2 Velocidades de datos del puente por encima de 11 Mbps

Los puentes de radio 802.11 son un regalo desde cualquier punto de vista cuando se trata de conectar dos o más sitios remotos. Tienen dos beneficios adicionales importantes, que son la capacidad de desplegarse con gran

rapidez, además de que se pueden desplegar con prácticamente ningún recurso dedicado a la licencia por parte del usuario final y a otras aplicaciones (además de, los permisos de construcción que se requieren) el resultado parcial de esto es que algunos clientes desearán obtener el valor y simplicidad de un puente 802.11, pero que tenga, velocidades de datos por arriba del estándar de 11 Mbps.

9.3.3 Reciclaje de canales

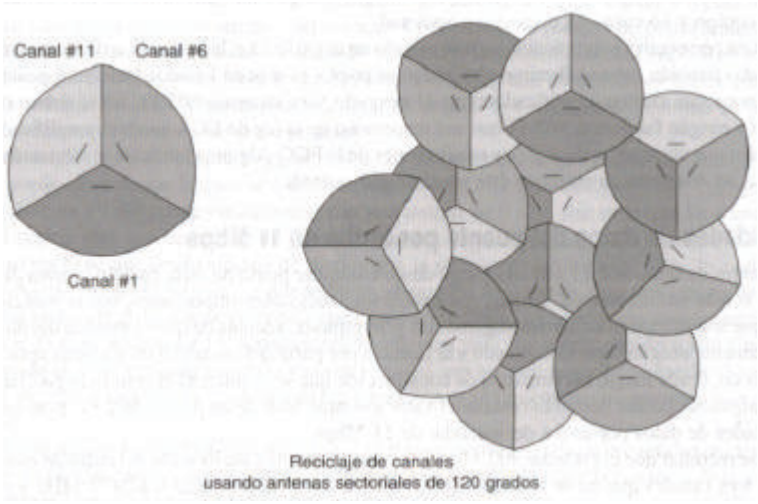

Figura 15. Ejemplo del reciclaje de canales

Uno de los enfoques más antiguos y más elegantes para maximizar la cantidad de canales disponibles en un puente 802.11 es el reciclaje de canales. La figura proporciona una muestra de la forma en que se pueden reciclar los canales de forma que se pueda cubrir un área muy considerable, incluso cuando sólo se cuenta con tres canales que no se traslapan.

La asignación de canales de tal forma que no afecten a las células adyacentes es muy importante. Es también crítico el uso de la cantidad adecuada de ganancia en las antenas. Demasiada ganancia puede ocasionar la pérdida de energía en un canal adyacente, o dos células arriba. Los cálculos de la pérdida de ruta que se llevan a cabo en las primeras etapas de planeación de células deben indicar al menos una pérdida de 10 dBm en un área en donde pueden recibir frecuencias comunes. Muy poca ganancia puede tener el mismo efecto. La planeación correcta del área física además de un entendimiento del desempeño de la antena y la configuración del radio, deben estar confirmados por una evaluación en sitio.

Las conexiones (la obtención de datos desde y hacia el área de cobertura) se deben considerar cuando se planee la frecuencia. Para muchos despliegues, las conexiones a través de cobre tienen la ventaja de liberar un canal de radio. Para los despliegues en donde existen menos de tres canales se pueden usar de forma satisfactoria. y cuando existen probabilidades mínimas del requerimiento de velocidad adicional en el futuro, el uso de uno de los canales para la conexión es efectivo en costo y relativamente fácil de implementar.

10. DISEÑO DE LA RED LAN INALÁMBRICA DE LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR (UTB), USANDO EL ESTÁNDAR 802.11B IEEE.

El diseño de Wi-Fi que realizaremos para la Universidad Tecnológica de Bolívar está basado en diferentes ítems que nombraremos uno a uno a continuación, pero antes expondremos lo que requerimos para la escogencia de los equipos en nuestro diseño. Las consideraciones que buscamos cumplir en el diseño para la UTB están en los siguientes puntos:

Buscamos cubrir toda el área de la UTB

Se le quiere entregar a cada usuario un máximo de 32 Kbps de bajada para la realización de sus operaciones (transferencia de archivos, Internet, correo, demás aplicaciones)

Se requiere la ubicación del o de los AP en puntos estratégicos

De acuerdo a lo anterior procedimos a analizar las consideraciones principales para la escogencia de los dispositivos y demás factores que intervienen en nuestro diseño.

10.1 Despliegue Wi-Fi en la UTB

El primer paso a dar en un proyecto es puntualizar los objetivos específicos y luego trazar un plan para conseguirlos. Estos objetivos variarán de acuerdo a las siguientes características:

Designación de áreas

Planeación de la capacidad

Planeación de la cobertura: Evaluación en el sitio

10.1.1 Designación de áreas

La designación del área, corresponde a los lugares que tendrán cobertura dentro de la universidad. Designaremos que la red se extenderá por toda el campus de ternera.

Para seguir uno de los factores importantes en los proyectos que es el presupuesto, el cual sabemos que no es fácil de conseguir, un proyecto piloto es la solución, si lo que se quiere es “probar el funcionamiento”, y evaluar las fugas de gastos y recursos para el proyecto, la veracidad en la estimación del presupuesto y la recuperación en la inversión.

Además es preciso que se reconozca que Wi-Fi tiene una curva de aprendizaje (por lo nuevo de la tecnología) y este proyecto piloto puede servir como un entrenamiento muy valioso.

El proyecto piloto lo hemos considerado como una optimización de la red, y como una opción que puede o no escogerse en el momento de implementar la red en la universidad.

10.1.2 Planeación de la capacidad.

Ya definida la estrategia de despliegue, el siguiente paso es la definición del nivel de servicio WLAN que se va a proporcionar.

Para determinar el numero de usuarios que se pueden conectar a los puntos de acceso de la red Wi-Fi, nos basaremos en el tamaño y la forma del área de cobertura. Como el medio de transmisión es inalámbrico, la cantidad de usuarios en un área de cobertura determinada, puede variar enormemente en la medida en que estos entren y salgan de esta. Y esto sin tener en cuenta las interferencias del medio. Por lo tanto las anteriores razones son suficientes para afirmar que la capacidad que tendrá la WLAN será una aproximación.

La planeación de la capacidad está destinada para funciones como, el acceso a internet, correo y transferencia de archivos en una base de datos. La transferencia de paginas web con muchas imágenes (o una videoconferencia) requiere de una cantidad sustancial de ancho de banda, digamos 300 Kbps, por lo que ésta aplicaciones en un caso de necesidad, deberá obtenerse con la configuración de los AP, dándoles priorización a los que lo requieran. Debido a que los puntos de acceso Wi-Fi compatibles con 802.11b proporcionan cerca de 11 Mbps de capacidad de salida agregada (esto garantizado por el fabricante de los equipos que intervienen), la cantidad de usuarios por punto de acceso se determina con una simple división entre la capacidad de salida del

AP y la velocidad de datos requerida para las aplicaciones de los usuarios. Para nuestro diseño consideraremos un máximo de 300 usuarios distribuidos en diferentes zonas (posteriormente se hará una presentación de éstas zonas y el numero de usuarios en ellas), conectados al tiempo, un número que sobrepasa el valor real, por la poca afluencia de portátiles en la universidad y las actividades que más frecuentemente se realizan en ella. Por ésta razón también buscamos hincar la necesidad de los equipos inalámbricos e incentivar el uso de la Internet y promover la búsqueda de información por parte de los estudiantes de una manera más cómoda y rápida, sin tener que dejar otras actividades.

Los cálculos de la capacidad de cada usuario, por zonas se realizará en la sección de ubicación de los AP en donde se especificarán mas detalladamente las zonas.

10.1.3 Planeación de la cobertura: Evaluación en el sitio

Como ya sabemos, que las ondas RF atraviesan paredes pero la señal pierde fuerza al hacerlo, y que algunos movimientos sutiles y cambios en la posición pueden tener un impacto tremendo en la forma en que se recibe la señal; además la señal se debilita a medida que se aleja del transmisor; cuando la señal está dentro de frecuencias similares pueden interferirse; y que al igual que las ondas visibles pueden ser obstruidas, causando la perdida de la señal.

Consideraremos los anteriores para le evaluación en el sitio (Campus de Ternera de la UTB). Así como la planeación de la capacidad se hizo para darle a los usuarios lo que necesitan, la planeación de la cobertura y evaluación en el sitio es proporcionarles lo que necesitan donde lo necesitan.

Para la evaluación del sitio se hizo necesario reunir información, para poder recomendar en donde colocar los puntos de acceso y el tipo de antenas que se debe usar. También se tuvo en cuenta el diseño de las diferentes áreas donde se piensa dar cobertura en la universidad, como lo son: los edificios de aulas 1 y 2, las cafeterías, la parte de Bienestar universitario, malokanet, las oficinas de rectoría, el auditorio, biblioteca y las áreas sociales que frecuentan los estudiantes, profesores y demás personal en la UTB, basados en planos generales además de una revisión directa. Se identificaron los materiales con que fueron construidos los edificios, los cuales son cemento o concreto con varillas de acero de soporte, ventanas de vidrio con marco de aluminio, oficinas cubiculares de madera en las decanaturas y demás oficinas. Se observaron bajos patrones de trafico inalámbrico en el edificio, solo comunicaciones celulares que no afectan la operación de Wi-Fi por estar ubicadas en un rango de frecuencias distinto al de 2.4 Ghz. Las barreras que aparecieron en los edificios y demás áreas de la UTB son relativamente bajos para las frecuencias en las que trabajaremos, por lo que no son consideradas de alto grado de interferencia y así se nos facilita el diseño El análisis de las barreras se hace

posible mediante el análisis del diseño de interiores y exteriores de las instalaciones de la UTB.

10.1.3.1 Diseño de interiores y exteriores.

Cuando se hizo el análisis de la forma como están construidas las diferentes zonas de la UTB, que entran en la cobertura de la red Wi-Fi, nos encontramos que para determinados casos la forma en que estas fueron diseñadas, favorecen o entorpecen la comunicación en la red; además es notorio que en la UTB existen más zonas abiertas en las que el personal se encuentra, ya que los salones de clases y laboratorios son para esa actividad y en la biblioteca, ya existe una red cableada que soporta gran parte de uso para los estudiantes, entonces nuestra red inalámbrica va más hacia las zonas abiertas que la cerradas. Continuando con los factores que intervienen en el medio para el rendimiento de la red, encontramos que en los casos en que la favorecen podemos citar lugares abiertos, oficinas cubiculares, dentro de los salones de clase y demás lugares donde no existen construcciones con materiales densos que pueden contener metal en su estructura ni construcciones que pueden desviar las señales (trayectorias múltiples). Entre los sitios desfavorables están las paredes de los salones y oficinas que van del piso al techo como principal obstáculo de la onda, ya que las superficies metálicas no son casi nulas en la construcción del campus, pero nos preguntamos; aunque las señales de 2.4 Ghz que usa 802.11b son capaces de atravesar paredes, ¿por qué las

seguimos considerando obstáculos?, pues, siempre se absorberá energía cuando la señal traspase una barrera y esto no es lo que se quiere.

Para la ubicación de los Ap tuvimos en cuenta los siguientes factores:

Evitar la penetración de paredes exteriores que degradan la señal. Cuando se presenten estos casos, se colocaran las antenas en la parte exterior del lugar donde se encuentre el AP.

En entornos abiertos se consideró una atenuación baja, como es el caso de las oficinas curriculares, cuartos entre paredes de vidrios como biblioteca y demás espacios abiertos que conocemos en la UTB.

Se permite la penetración de paredes interiores hechas con materiales de baja densidad como el yeso, cemento, e incluso bloques (con mayor precaución).

Evitar completamente la penetración de paredes hechas total o parcialmente de metal puesto que este material induce las trayectorias múltiples y la obstrucción completa de la señal. En este caso no tuvimos mucho problema, debido a que en la UTB este caso ya se había dicho que es nulo.

Como podemos ver, lo dicho anteriormente fueron las consideraciones y la planeación que se hizo para realizar el proyecto, lo que constituye el primer paso, el cual esta soportado por una verificación real, que se basa en los planos de la UTB que contienen las ubicaciones de cada AP teniendo en cuenta la evaluación en el sitio. Estos planos están anexos a la monografía.

Para los AP se utilizaran antenas omnidireccionales por el patrón de cobertura circular que ofrecen. Así se podría ver una zona muy extensa (hablamos de muchas decenas de metros) de oficinas en donde se requieren tres AP con antenas omnidireccionales para dar cobertura a todos los usuarios, como se ve en la figura 15, caso que no se presenta en la UTB en donde las áreas de oficina no sobrepasan los (3000 $m^{2)}$[16].

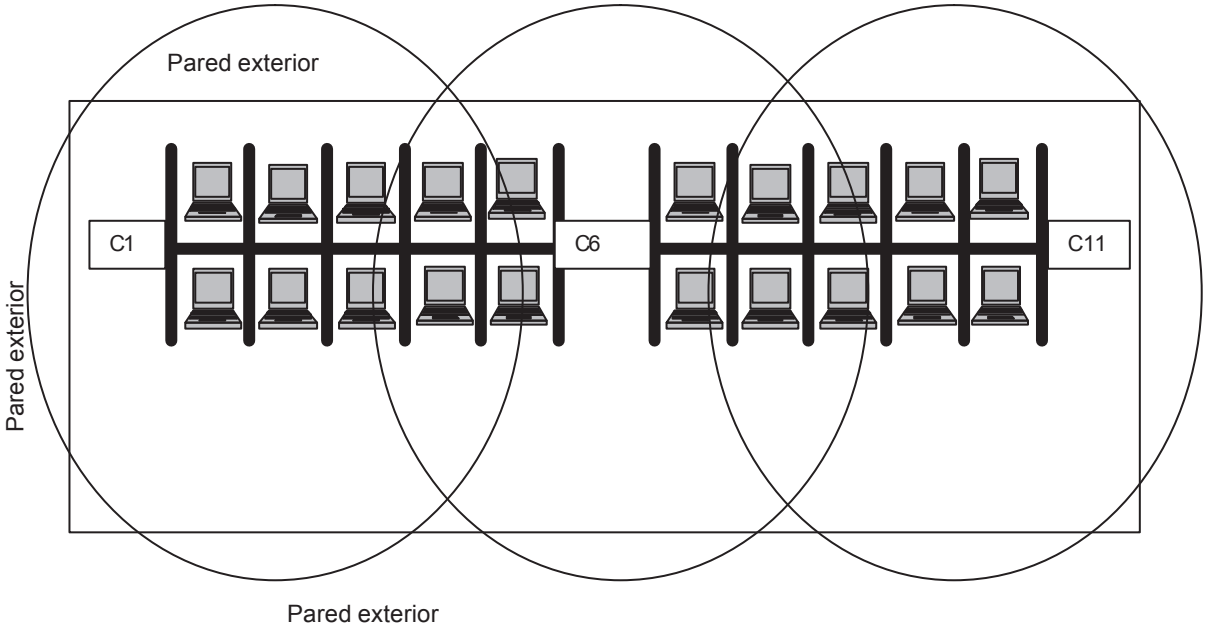

Figura 16. Vista de arriba de un centro de oficinas curriculares extensas

Como se muestra en la figura 15, en la banda de 2.4 Ghz existen tres canales no traslapados, el C1(2.412 GHz), el C6(2.437 GHz), el C11(2.462 GHz), para 802.11b. Podemos ver que en este caso la interferencia entre canales no es problema, lo cual nos simplifica el despliegue.

[16] Datos obtenidos por una tabla que nos facilitó la dirección de Ingeniería civil. Esta tabla estará disponible en los anexos.

10.1.3.2 Ubicación de los puntos de acceso

En esta parte se hizo la selección de los mejores sitios para colocar los puntos de acceso y antenas (lugares estratégicos en donde se busque minimizar costos y sacar provecho de los recursos), y encontramos como ubicación de un AP principal en Malokanet, con antenas omnidireccionales en la parte externa al recinto cerrado, que proporcionan celdas circulares que maximizan el área de cobertura. La colocación de los AP en los techos hace que los puntos de acceso estén lejos de la personas, minimizando el contacto intencional o no intencional. Preferimos colocar las antenas externamente, con el fin de brindar una mayor cobertura en outdoor (zonas abiertas con respecto a la ubicación de las antenas transmisoras). Esto hace que se alejen las antenas del AP una pequeña distancia y provoca pédidas en el cable, que no son de muchos dB[17], pero aun así éste dato lo podemos calcular.

Las antenas están en la parte exterior de malokanet y estarán alejadas máximo 5 metros del AP, por lo que el cálculo de la pérdida en el cable se puede calcular de acuerdo a la siguiente tabla[18]:

Tabla 6. Pérdida en dB por cada 100 m de diferentes tipos de cable coaxial

Cable	Pérdida en dB/100 m
LMR-200	54.2

[17] Especificado en el "Manual de redes inalámbricas" de Neil Reid y Ron Seide
[18] La información en las tablas se encuentra en el material del Ing. Jaime Rueda Rivera; ponente del módulo de redes Lan-Man-Wan, del "Minor comunicaciones y redes"

LMR-240	41.5
LMR-400	21.7
LMR-600	14.2
LMR-900	9.58
LMR-1200	7.27
LMR-1700	5.51

Para extender las antenas del AP utilizaremos el cable coaxial LMR-400, por lo tanto para 5 metros de distancia, tendríamos una pérdida de 1,085 dB.

Como se había dicho la colocación de los AP es fundamental, por esto se puede tomar como segunda opción cuando no es posible la colocación en cielos rasos, ubicarlos en las paredes. Cuando se instalan antenas omnidireccionales, los puntos de acceso Wi-Fi de 2.4 GHz montados en la paredes pueden cubrir dos habitaciones.

Para cumplir con los objetivos de cobertura y de capacidad de la red por usuarios decidimos colocar tres Ap adicionales en zonas relevantes con cierto número de usuarios. Estas zonas son:

Biblioteca: 30 usuarios conectados a la vez.
Rectoría y Dirección de Ingeniería de Sistemas: se suponen unos 20 usuarios conectados simultáneamente.

Edificio de Aulas 2: Aquí se encuentran los laboratorios de Control Automático, Electrónica y de Física; por lo que se suponen 30 usuarios conectados al tiempo.
Otros 220 usuarios distribuidos, entre zonas de campo libre como cafeterías, kioscos y espacios cercanos a malokanet.

Estas consideraciones son hechas, buscando un acercamiento a la utilización real de los PC portátiles y que además la red está más dirigida hacia las zonas abiertas, ya que existe una red cableada en la UTB que brinda los diferentes servicios que brinda nuestra red Wi-Fi. Además no tendrá mucho uso la red en espacios donde se cumplen otras funciones (como por ejemplo, aulas de clases, prácticas de laboratorio, biblioteca, zonas deportivas, etc.).

Ahora bien, la ubicación exacta de los AP adicionales será la siguiente:
En la biblioteca, en el segundo piso (espacio de mesas para trabajar en grupo), se ubicará un punto de acceso, que realmente trabajará como un mini repetidor, ya que el AP que seleccionamos tiene esa función. El AP estará sobre el cielo raso cerca de las paredes de vidrios de la biblioteca.

Entre rectoría y Dir. De Ingeniería se Sistemas (zona especificada en el plano), se ubicará otro mini repetidor de la misma familia que el anterior y los demás AP que se utilizarán para ésta función.

Por último otro repetidor, estará ubicado en la parte externa al laboratorio de Control (Edificio Aulas 2).

El AP principal de Cisco, estará ubicado en Malokanet.

Ahora, la capacidad total de bajada para cada usuario se garantizará por zonas y por el número de usuarios.

Para la zona de la biblioteca, en donde habíamos supuesto 30 usuarios conectados al tiempo, se está manejando de acuerdo a lo que brinda el AP D-Link 700 en indoor (unos 25 a 30 metros de radio), una capacidad de salida de 1 Mbps, pero como en realizar, en esa zona no se encuentras barreras desfavorables para la señal se tendrá mayor capacidad; pero para garantizar nuestro diseño tomaremos como si fuera 1 Mbps; entonces si a cada usuario le entregamos 32 Kbps total para las diferentes aplicaciones, entonces estaríamos necesitando un total de 0.937 Mbps, por lo que 1 Mbps, soporta los 32 Kbps para los 30 usuarios.

El mismo cálculo lo hacemos para el edificio de Aulas 2, en donde también se consideran 30 usuarios y también tenemos el mismo caso con una capacidad de salida del repetidor de 1 Mbps; por lo que los cálculos también nos garantiza la capacidad total por usuario.

Para el caso de la zona entre rectoría y dirección de Ing. de Sistemas, tenemos 20 usuarios conectados al tiempo y un total también de 1 Mbps; entonces aquí sólo necesitaríamos 0.625 Mbps para garantizar los 32 Kbps por usuarios. Aquí nos sobra unos Kbps de ancho de banda para ser utilizado en casos que lo requiera. Y en éste caso sólo se debe realizar una configuración del AP.

Por último la zona más concurrida y a la que dedicaremos un mayor ancho de banda por la posibilidad de extensión, es la demás zona abierta y cercanas a malokanet, en donde hemos supuesto unos 220 usuarios conectados al tiempo. En ésta zona, se está brindando por el AP principal un ancho de banda en capacidad de transmisión de 11 Mbps hasta los 244 metros de radio; por lo que quedaría libre un total de 4.125 Mbps, ya que los 220 usuarios tomarán sólo 6.875 Mbps, garantizando los 32 Kbps para cada uno.

Vale anotar algo respecto al auditorio y bienestar universitario; en bienestar por ejemplo, no hay muchos sitios cerrados, por lo que cabe dentro de los 244 metro que brinda capacidad total de 11 Mbps, y las pequeñas oficinas están separadas en gran parte por vidrios, por que la señal a 2.4 GHz de frecuencia puede fácilmente pasar. Si es necesario en un futuro podría colocarse un AP en bienestar universitario, pero ahora no se es necesario, teniendo en cuenta que éste es un proyecto piloto.

Ahora, el caso del auditorio, es por poco uso, éste sitio está destinado para actividades predeterminadas, y si en alguna necesidad se requiere podría instalarse otro mini repetidor, que sería suficiente para brindar los Kbps por usuario que se deseen (éste factor se manejará en la configuración del AP).

10.1.4 Selección del fabricante para los puntos de acceso y los adaptadores de cliente

La selección de los adaptador de cliente es muy sencilla; principalmente se trata de decidir cual es la plataforma en que el adaptador de cliente residirá. Si se trata de un computador de escritorio, entonces se tendrá que instalar una tarjeta PC; un computador portátil con una ranura PCMCIA, requiere de una tarjeta de red de este mismo tipo.

La selección del AP es de requerimientos de nuestro diseño, pues bien, es obvia la razón por la que se debe tomar un buen fabricante; partiendo de que un AP económico más tarde puede salir caro, por que puede brindar poca garantía, tiene menos aplicaciones de configuración y podría limitar la futura extensión de la red. De acuerdo con la investigación de la compañía Dell'Oro, Cisco System es el fabricante mas grande de equipo 802.11 para el mercado empresarial, como se muestra en la figura 16.

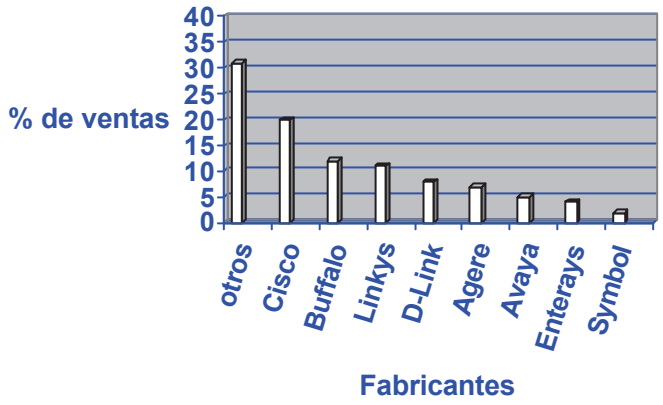

Gráfico 1. Repartición del mercado 802.11 en el ámbito empresarial

Como podemos observar Cisco es el fabricante de dispositivos 802.11 mas competitivo en el mercado empresarial, y aunque no es el menos costoso, cumple con la mayoría de las siguientes condiciones: desempeño, confiabilidad, interoperabilidad, seguridad, experiencia, estabilidad financiera y por ende costo. Por razones obvias Cisco debe ser considerado fabricante preferido por su amplia experiencia en redes. Aunque el precio no es la medida principal de la comparación de equipos 802.11, sigue siendo un factor que no se puede ignorar. La tabla 6 compara el precio del equipo de los fabricantes principales.

Tabla 7. Precios de productos de principales fabricantes de 802.11

Fabricante	Producto	Precio US
Agere System	World PC Card –Gold	$119
Agere System	USB Client-Gold	$169
Agere System	AP-500 (integrated PC Card Radio)	$495
Agere System	AP-200	$199

Agere System	Remote Outdoor Router (ROR-1000)	$1345
Agere System	Central Outdoor Router (COR-1100)	$1695
Alvarion	PC Card	$155
Alvarion	AP-DS. 11 Indoor	$575
Alvarion	Remote Bridge	$2345
Alvarion	Base Unit	$2650
Buffalo	Wireless LAN Card	$119
Buffalo	USB client	$179
Buffalo	AirStation Pro	$549
Cisco	350 Series PC Card	$169
Cisco	350 Series Access Point	$749
Cisco	1200 Series Access point	$850
Cisco	1200 Series. 11b Mini-PCI	$149
Cisco	1200 Series Access Point with. 11b Mini-PCI	$999
Cisco	1200 Series 11a. Radio Module	$499
3Com	3Com Workgroup Bridge	$349
3Com	3Com AP 8000	$749
3Com	3Com AP 6000	$499
3Com	3Com AP 2000	$199
3Com	3Com Building-to-Building Bridge	$1095
D-Link	PC CardBus Adapter	$90
D-Link	802.11a Wireless PC Card	$170
D-Link	802.11a Wireless Access Point	$399
D-Link	5 GHz/2.4 GHz Dual Band Wireless Access Point	$499
Enterasys	High Rate PC Card	$149
Enterasys	R2 Wireless Access Platform (PC Card sold separately)	$1349
Enterasys	Access point 2000	$849
Enterasys	R1 Wireless Access Point	$399
Intel	PRO/Wireless 2011B LAN PC Card	$112
Intel	Access point	$449
Intel	PRO/Wireless 5000 LAN Dual Access Point	$649
Linksys	Instant Wireless Network PC Card	$128
Linksys	Wireless Ethernet Bridge	$190
Linksys	Instant Wireless Network Access Point	$220
Linksys	Instant Wireless Network PC Card	$210
Linksys	Instant Wireless Access Point	$500
Proxim	PC Card	$149
Proxim	Access point	$695
Symbol	Ethernet AP	$899
Symbol	AP 4121 Access Point	$999
Western Multiplex	Tsunami 10BaseT Wireless Ethernet Bridge	$6995

De acuerdo a todas las notas anteriores, se justifica el porque utilizamos como AP principal uno de Cisco; éste es de la serie 350, cuyas características estarán en los anexos. Y para los repetidores utilizaremos AP D-Link 700, por su bajo consto y además son para darle ganancia a la capacidad por zonas pequeñas.

10.1.5 La evaluación física en sitio

Esta parte se considera en el momento en que se decide instalar la red, se requiere hacer pruebas en todas las ubicaciones planeadas antes de hacer la inversión, debido a que una cosa es lo que esta escrito y otra lo que puede ser en la realidad. Se colocan los puntos de acceso y las antenas seleccionadas en los posibles lugares temporalmente mientras se hacen las mediciones, luego cuando se encuentre el lugar optimo se marca el sitio donde irá el AP con alguna cinta brillante que no nos haga perder de vista este lugar.

Para este propósito se requiere de una herramienta de evaluación en sitio de algún fabricante. La mayoría de los fabricantes Wi-fi ofrecen, junto con las utilidades de los adaptadores de cliente, herramientas para la evaluación en sitio que tienen capacidades distintas. Estas herramientas reportan el punto de acceso con el cual esta asociado el cliente, mostrando datos como: la fuerza de la señal y la velocidad de datos que soporta además del nivel de ruido en el ambiente. Algunas herramientas de evaluación en sitio incorporan una prueba

ping para medir el numero de paquetes IP que se pierden durante una transferencia.

La documentación respecto a las ubicaciones de los AP, es un aspecto a priori debido a que esa información sería muy necesaria para una referencia futura sobre como fue construida la red, además para propósitos de solución de problemas y seguridad.

Cuando se hace la evaluación en sitio se deben tener en cuenta las capacidades de los adaptadores clientes, que por lo general son de distintos fabricantes y por lo tanto tienen variaciones en la potencia de transmisión de aproximadamente. Los distintos dispositivos de cliente proporcionan diferentes ganancias en la antena, lo cual agrega una variación en general aún mas grandes en las capacidades de cliente. En las áreas en las que es probable que se incluyan tipos de clientes distintos, la planeación se hará usando el denominador común mas bajo, es decir los clientes con capacidades mas bajas.

10.2 Administración de la red Wi-Fi de la UTB

Cuando se haya hecho el despliegue de la red Wi-Fi en la universidad, ésta deberá ser administrada de la misma forma que una LAN cableada. Los AP deben contar con una interfaz de administración, con un explorador y una

interfaz de línea de comandos (Command-Line Interface, CLI) en donde se puedan escribir archivos de comando para automatizar tareas en un numero grande de dispositivos. Además de esto, deben contar con soporte para el Protocolo simple de administración (SNMP, Simple Managment Protocol) requerido para la operación con el Software de administración de red (Network Managment Software, NMS), por ejemplo, OpenView de Hewlett Packard y Unicenter de Computer Asociates que se usan en redes cableadas.

10.2.1 Mantenimiento de la infraestructura Wi-Fi

Un mantenimiento de la infraestructura Wi-Fi, requiere que se actualicen constantemente el firmware o archivos de configuración. Esto significa que se realizaran actualizaciones de software frecuentemente en todos los AP desplegados.

Las características de la interfaz de explorador de los AP permiten replicar una configuración de un solo AP en todos los demás AP, descargar una actualización del firmware desde un servidor centralizado al cual esta dirigido el AP mediante un enlace proporcionado por un servidor BOOT-PC o DHCP y cambiar las contraseñas e información SSID.

10.2.2 Supervisión de la Infraestructura

Los AP proporcionan listas de asociación y registros detallados de manera que el supervisor de la red pueda estar al tanto de forma continua de la carga de usuario y ancho de banda en cada dispositivo. De la misma forma en que la evaluación en sitio verifica y ayuda a refinar el plan de capacidad, con los AP, los datos del estado del sistema están disponibles a través de la CLI, el explorador o por medio de un MIB (Bases de información de administración).

CONCLUSIONES

Es un hecho que en situaciones en las que el cableado es una opción impráctica, las tecnologías inalámbricas nos pueden sacar de aprietos. En lugares donde los cables son antiestéticos, y es imposible cablear, en conexiones de redes temporales, que solo serán utilizadas en un lapso de tiempo, en locales arrendados, circunstancias como estas hacen imprescindible la opción inalámbrica.

En cuanto a la elección de la tecnología inalámbrica que se debe implementar, cada tecnología cuenta con diferentes patrones de funcionamiento que para cada aplicación pueden ser muy útiles. Por ejemplo, en entornos pequeños como en los que se dan aplicaciones para el hogar, en oficinas pequeñas, y otras aplicaciones personales; HomeRF y Bluetooth, pueden competir y ofrecer ventajas importantes debido a las velocidades de datos y la cobertura que estos manejan, propias para estos casos.

Si se pasa a un plano mas extenso, como campus y zonas de áreas muy grandes, y que además requieras ciertos tipos de aplicaciones, como es en nuestro caso, la Universidad Tecnológica, las características de los dispositivos de estas tecnologías se quedan cortas ante la gran demanda de usuarios y aplicaciones que se requieren. En estos casos, no se duda en escoger la implementación del estándar IEEE 802.11x, que fue desarrollado en este

trabajo en su mayor parte, en torno al 802.11b, debido a su amplia existencia en el mercado de productos Wi-Fi. Este estándar es capaz de entrelazar estaciones de trabajo que se encuentren distantes hasta 30 metros, con velocidades de datos máxima de 11 Mbps compartida, características suficientes para que los estudiantes y profesores se sientan cómodos en el sitio que quiera (campus ternera), accediendo a las bases de datos y gozando del servicio de Internet.

La conformación de esta red, es posible, contando solamente con la distribución de los puntos de acceso, en los lugares que se indicaron para dar cobertura a todo el campus universitario, las antenas que hacen posible el envió y recepción de los paquetes de información y un computador portátil (con el que se supone cuentan los usuarios), con su respectivo dispositivo cliente, es decir, la tarjeta de red, que para este caso es la PCMCIA compatible con Wi-Fi.

La red está conformada de manera que se puedan aprovechar al máximo las prestaciones que nos brindan los dispositivos Wi-Fi con el estándar 802.11b. Estos dispositivos cuentan con muchas opciones que deben ser configuradas por el autor del despliegue de la red, las cuales permiten una comunicación confiable, estable y segura. Por ejemplo, opciones como RTS/CTS que eliminan los inconveniente que imponen los nodos ocultos, y en cuanto a la seguridad la selección de un estándar de seguridad como el 802.11i que

corrige los errores de otros mecanismos mas rudimentarios como el WEP, haciendo que la comunicación no sea alterada o corrompida por usuarios no autorizados.

Otro factor que se tiene muy en cuenta para la implementación de una buena red, radica en la posibilidad de tener medios para dar prioridad a cierta información dentro de la red, permitiendo que la red restrinja en cierta forma el uso de los canales que son utilizados por las estaciones de trabajo (que usan la democracia de CSMA/CA). La calidad de servicio QoS es la que hace esto posible, y además de esto se agrega que la calidad de servicio en las tecnologías inalámbricas no tiene aun un alto poder; debido a lo nuevo de las tecnologías y a que está en aprobarse el estándar IEEE 802.11e, que establece los apuntes necesarias para el QoS en las WLANs. Aun así, debe ser muy tenida en cuenta en el diseño, debido a que en un ambiente universitario, es muy probable que ciertas personas deban acceder a información con prioridades más que otras, como es el caso de un alumno que pone a sufrir la red bajando un archivo de música con el popular Kazzaa, y en otra parte de la célula de cobertura, se encuentre el decano de Ing. Electrónica, bajando un archivo o un programa para fines académicos. Este interrogante se soluciona proporcionándole QoS a la red, con métodos de priorización de paquetes descritos en el capítulo que maneja éste tema a fondo.

RECOMENDACIONES

- Para la seguridad de nuestra red se recomienda utilizar un servidor de autenticación RADIUS e implementar el esquema de autenticación de 802.1x, haciendo posible que se dé tanto la autenticación del usuario como de la LAN.

- Para prolongar la vida útil de los dispositivos Wi-Fi, activar el modo de ahorro de energía desde el software de configuración de estos.

- Para garantizar la interoperabilidad entre todos los dispositivos Wi-Fi de la red, se deben ajustar con características de funcionamiento iguales, como frecuencia de operación, velocidad de datos, y otros modos operación como RTS/CTS, encabezado corto, fragmentación de tramas.

- Para que la red funcione correctamente, cuando se traslapan dos células de cobertura de dos AP diferentes, se recomienda que estén ajustados para trabajar en canales de frecuencias diferentes de los que se encuentran disponibles (1, 6 y 11), para evitar interferencias.

- Se recomienda tener en cuenta los materiales de construcción que se utilicen en construcciones futuras, que puedan afectar e interferir en la transmisión de las señales de 2.4 GHz de los AP.

- Para la ubicación de las antenas de los puntos de acceso que puedan ser instalados en un futuro se recomiendan los exteriores, como techos para que la señal no sea interferida por obstáculos mayores.

- Para mejorar el diseño se puede pensar en utilizar dispositivos Wi-Fi que sean también compatibles con el estándar 802.11a que ofrece mas velocidad de datos en los AP y dispositivos de cliente. Para esto se debe hacer un replanteamiento del presupuesto que se va a disponer para la red.

- Para que el aprovechamiento de las bondades que ofrece Wi-Fi sea máximo se recomienda a la universidad comprar mas ancho de banda al ISP para las aplicaciones de Internet.

BIBLIOGRAFÍA

DORNAN, Andy. Guia práctica para usuarios : WAP. Madrid: Ediciones Anaya Multimedia, 2001. 31 p. 219 p.

BLACK, Uyless. Tecnologías emergentes para redes de computadores. 2 ed. México: Prentice Hall Hiapanoamericana, S.A., 5 p. 123 p. 132p.

TOMASI, Wayne. Sistemas de Comunicaciones Electrónicas. 2 ed. México: Prentice Hall Hiapanoamericana, S.A., p 377-382, p 477-495 p 692-700

REID, Neil. y SEIDE, Ron. 802.11 (Wi-Fi) : Manual de redes inalámbricas. México: McGraw-Hill Interamericana Editores , S.A. DE C.V., p 65-78, p 91-154, p 175-203, 209 p., p 217-242, p 243-253, p 268-281.

RUEDA, Jaime Antonio. Minor Comunicaciones y Redes 2003-2004 : Modulo Redes Lan – Man – Wan. Cartagena.

AGUANCHE, Leonel Ramón. Diseño del sistema dinámico de conectividad inalámbrica para servicio de Internet en la Corporación Universitaria Tecnológica de Bolívar. 2004

LLORENTE, Jose Alejandro. Diseño e implementación de un prototipo de red inalámbrica para la CUTB.

Referencias en la WEB

www.cisco.com

www.3com.com

www.D-Link.com

www.wirelessmundi.com

www.LinkSys.com

http://www.mailxmail.com/curso/informatica/wifi/toc.htm

www.proxim.com/learn/library/whitepaper/wireless_security.pdf

www.wi-fi.org

http://pof.eslack.org/wireless/

http://www.matarowireless.net

ANEXOS